सत्यमेव जयते

DSIR

DEPARTMENT OF SCIENTIFIC AND INDUSTRIAL RESEARCH

ICRIER

Report on

The Role of Standards in Diffusion of Emerging Technologies Internet of Things (IoT)

Mansi Kedia
Richa Sekhani
Tanay Katiyar

Department of Scientific and Industrial Research (DSIR)
Ministry of Science & Technology, Government of India
October 2020

DISCLAIMER: *Opinions and recommendations in the report are exclusively of the author(s) and not of any other individual or institution including ICRIER. This report has been prepared in good faith on the basis of information available at the date of publication. All interactions and transactions with industry sponsors and their representatives have been transparent and conducted in an open, honest and independent manner as enshrined in ICRIER Memorandum of Association. ICRIER does not accept any corporate funding that comes with a mandated research area which is not in line with ICRIER's research agenda. The corporate funding of an ICRIER activity does not, in any way, imply ICRIER's endorsement of the views of the sponsoring organization or its products or policies. ICRIER does not conduct research that is focused on any specific product or service provided by the corporate sponsor.*

Table of Contents

List of Tables

List of Figures

List of Boxes

Acknowledgments

We are grateful to our project sponsor, the Department of Scientific and Industrial Research (DSIR), particularly the program head for A2K+ studies, Dr. Sujata Chaklanobis, for giving us this opportunity to present this report that provides a policy focus on the role of standards in diffusion of emerging technologies such as IoT. We are extremely grateful to Department of Telecom (DoT), the Bureau of Indian Standards (BIS), the Telecommunications Standards Development Society, India (TSDSI), the Telecom Engineering Centre (TEC), the Institute of Electric and Electronics Engineer (IEEE) and the Seconded European Standardization Expert for India (SESEI)for sharing detailed responses on several policy questions. Industry perspectives from the Broadband India Foundation (BIF), the GSM Association, Centers of Excellence (CoE) at NASSCOM, Confederation of Indian Industry (CII), India Electronic and Semiconductor Association (IESA), Samsung- Open Connectivity Foundation (OCF), Gaia Smart Cities, HP (Bhopal Smart City), Plant Connect and B&R Industrial Solution, Smart Control, Sensorise and Tech Machinery Labs for providing relevant ground realities. We are indebted to the members of the Project Guidance & Review Committee (PGRC), in particular, Dr. Sanjiva Prasad from IIT Delhi, Jitendra Kumar from BIS and Dr. Ashwani Gupta, Dr. Suman Mazumdar, Dr. Vipin Shukla & Dr. Kailash Petkar from DSIR, for their review comments and constant support We were honoured to invite the National Accreditation Board for Education and Training (NBIT) Delhi, the Indian Institute of Information Technology, Bangalore (IIIT-B), and the Institute of Technology (IIT), Delhi for providing the academicians perspective to the challenges of standardisation in India. We are also grateful to sector experts Mr. Deepak Maheshwari, Mr. PVG Menon, Mr. Kishor Narang and Mr. Sachin Gaur for sharing inputs that have shaped the analysis presented in this report

Finally, we are grateful to our team at ICRIER for their unending supply of wisdom and time, making ICRIER a delightful place to reflect on such an engaging and stimulating area of research. All errors of course remain our own.

List of Abbreviations

3GPP	3rd Generation Partnership Project
AIOTI	Alliance for Internet of Things
AIOTI	Alliance for Internet of Things Innovation
AIPL	Ascent Intellimation Pvt. Ltd
ANSI	American National Standard Institute
API	Application Programming Interface
ATL	Authorised Testing Lab
BIF	Broadband India Foundation
BIS	Bureau of Indian Standards
CAGR	Compound Annual Growth Rate
CII	Confederation of Indian Industry
COE	Centers of Excellence
CPIP	Cloud Portability and Interoperability Profiles
CPRI	Common Public Radio Interface
CTA	Consumer Technology Association
DDoS	Distributed Denial of Service
DSIR	Department of Scientific and Industrial Research
EFTA	European Free Trade Association
ENSIA	European Union Agency for Cyber security
EPSG	Ethernet Power link Standardisation Group
ESMIG	The European Smart Energy Solution Provider
ETSI	European Telecommunications Standards Institute
FDIS	Final Draft International Standard
FRAND	Fair, Reasonable and Non-Discriminatory
GDPR	General Data Protection Regulation
GIS	Geographical Information System
GISFI	The Global ICT Standardization Forum for India
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAMAI	The Internet and Mobile Association of India
IBSG	Internet Business Solutions Group
IDC	International Data Corporation
IDC	International Data Corporation
IEC	International Electro technical Commission of standardisation
IEEE	Institute of Electric and Electronics Engineer
IESA	India Electronic and Semiconductor Association
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IIOT	Industrial Internet of Things
IIT	Indian Institute of Information Technology
IOT	Internet of Things
IoT4SCTF	IoT for Smart Cities Task Force
IPR	Intellectual Property Rights
ISA	International Society of Automation

ISA	International Society for Automation
ISO	International Organization for Standardisation
ITU	International Telecommunication Union
LMLC	Low Mobility Large Cell
MEITY	Ministry of Electronics and Information Technology
MEMS	Micro Electromechanical Systems
MESA	Manufacturing Enterprise Solutions Association
MQTT	Messaging Query Telemetry Transport
NBIT	National Accreditation Board for Education and Training
NIST	National Institute of Standards and Technology
OAGi	Open Applications Group
OCF	Open Connectivity Foundation
OTA SM	Over-The-Air Subscription Management Standard
PPP	Public Private Partnership
PSN	Packet-Switched Networks
REC	Radio Equipment Control
RFID	Radio-Frequency Identification
ROOF	Real-time Onsite Operations Facilitation
RRF	Remote Radio Head
SBIPA	Software Based Intelligent Process Automation
SDO	Standard Development Organisation
SESEI	Seconded European Standardization Expert for India
SMB	Standardisation Management Board
SMPTE	Society of Motion, Picture and Television Engineers
SNAP	Standards National Action Plan
SSCC-CG	Smart and Sustainable Cities and Communities Coordination Group
SSIA	Singapore Semiconductor Industry Association
SSL	Secure Socket Layers
SSO	Standard Setting Organisations
STPI	Software Technology Parks of India
TEC	Telecom Engineering Centre
TLS	Transport Layer Security
TSDSI	Telecommunications Standards Development Society, India
TSN	Time Sensitive Networking
TTA	Telecommunications Technology Association
UPB	Universal Power line Bus
VESA	Video Electronics Standards Association
WLAN	Wireless Local Area Network
WWRF	Wireless World Research Forum

Executive Summary

The explosive growth in mobile devices and the increasing ubiquity of wireless connectivity has propelled the growth of IoT and its applications across several countries. With an increasing number of applications and devices, global IoT spending is expected to touch $1 trillion by 2023[1]. The IoT market in India was estimated to be USD 1.3 billion in 2017 and is likely to expand to USD 9 billion by the end of 2020[2], with an installed base of 1.9 billion units. However, for market forecasts to manifest into an economic reality, smooth standardisation of products and processes is critical.

The past decade has overseen the emergence of a fragmented and proprietary IoT ecosphere[3], with private companies trying to create niche markets and promoting their own 'Internet of Things[4]. Standardisation is essential for the deployment interoperable and secure IoT systems with plug and play opportunities for new solutions in the market. Several standard development organisations (SDOs), industry consortia and alliances, across the world, are working on standards for deployment of IoT. Over a hundred different bodies are currently involved in developing standards across verticals such as home/ buildings (ULC, KNX), manufacturing/ industry automation (eCl@ss, CLPA), healthcare (IHE, DICOM), energy (OASIS, SGIP), etc. as well as horizontal service and infrastructure requirements (IEEE, OneM2M, JTC1, IEC).

In India, BIS publishes IoT related standards under eight different working groups of the Electronics and Information technology (LITD) technical departments. The Telecommunications Standards Development Society, India (TSDSI) is an application specific SDO within the generic SDO jurisdiction. The Telecom Engineering Centre (TEC) provides support and advice to DoT on technology, spectrum and licensing related issues and produces standards related documents. TEC develops telecom product specification and interoperability (interface) specification for seamless working of telecom networks and devices. However, India's current contribution to standards development has been very limited. The ongoing efforts are also at a nascent stage and mostly driven by global companies operating in India.

Standards organisations operate in multiple formats. There is growing recognition among countries for the need to work together and establish good practices and enable broad-based participation in the standards development process. SDOs encourage participation in the development process by highlighting benefits such as increasing stakeholders' strategic and technical influence in an industry, while gaining early access to information on an evolving standard to be better placed when designing and introducing new products. However, benefits provided by SDOs are not uniformly attractive to all types of members with an interest in standards. SDOs are also governed in different formats. Some of their distinguishing criteria include (i) knowledge areas, (ii) membership guidelines including membership fees, (iii) norms, guidelines and good practices, (iv) ratification and (v) intellectual property rights (IPR).

The study provides a detailed discussion on each of these parameters revealing that governance structures and processes (like ratification, openness and membership fees to name a few) play a vital role in determining which standard makes it to the fore. This is further complicated by IPR regimes (which FRAND offsets to a great extent) which might impede the voices of start-ups and small-scale enterprises in shaping the narrative of lesser known but relevant standards While pre-screening of SSOs is important

---

1 IoT News (2019). "Global IoT spending to break $1 trillion by 2023 – fuelled by solid consumer and commercial adoption", June 14, 2019. https://www.iottechnews.com/news/2019/jun/14/global-iot-spending-break-1-trillion-2023-fuelled-solid-consumer-and-commercial-adoption/

2 Deloitte Analysis, NASSCOM https://www.wfeo.org/wp-content/uploads/stc-information/L3-IoT_Landscape-by-S_Malhotra.pdf

3 Darmois. S, Daniele. L, Guillemin. P, Heiles. J, Moretto. P and Van der Wees. A: IoT Standards Landscape – State of the Art Analysis and Evolution. https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609105C6.pdf

4 Basulto. D (2015). 3 reasons why the Internet of Things (still) doesn't make sense, The Washington Post.

for businesses and contributors to the standard development process, governments must ensure that stakeholders collectively gain from the benefits of participating in the process and catalyse technology development at the macro-level. The focus on governance of SSOs is particularly relevant to India as it prepares to transition from a follower to a contributor for emerging technologies such as IoT. Timothy Simcoe found that voluntary SSOs using a consensus process had become increasingly politicized, crippling standards production for the Internet between 1993 and 2003.

In our case study analysis of IoT solutions developed and deployed in India we cover examples for industrial and consumer IoT as well as smart cities.

Industrial IoT: Industrial IoT (IIoT) is a subset of IoT that uses sensors, computers and networks which interact with their environment to generate data for optimization of industrial applications. Our interaction with IIoT companies establishes the growing recognition amongst solution providers on the use of standards to establish interoperability and data security across their services in India. The standards used for communication across machine software, hardware, data transmission and data security for IIoT in India include OPC-UA, a new standard being rapidly adopted for Industry 4.0.[5]The standard is open source and available free of cost. With OPC-UA, Ethernet time sensitive networking (TSN), real time data for automation and robotics application would be possible. This will provide vendor independent end-to-end interoperability into field level devices for all relevant industry automation use-cases. Currently, the adoption of OPC-UA solutions is limited only to large scale companies in India. The small and medium enterprises lack awareness on availability of such standards. Power link is a standard for data transfer adopted by IEEE under IEEE 61158. For safety-critical data, the Ethernet Power link can be expanded with the open SAFETY protocol. Some other important standards being used in India are Industrial Internet Reference Architecture V 1.9, ISA95 Enterprise-Control System Integration, ISA88 Batch Control and ISA/IEC 62443 Cybersecurity Certificate Programs, besides other prominent standards adopted by IEEE. The adoption of these standards for Industrial IoT is however limited. For instance, the baggage of old machinery and huge costs associated with smart manufacture are limiting Industrial IoT in India. Finally, while the world is seeing standards around combination technologies such as Artificial Intelligence (AI), Machine Learning (ML), Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), etc.; India is still to see its wide adoption in IIoT applications. These technologies add new dimensions to IoT and expand its potential. There are various formal standards bodies such as IEEE, Video Electronics Standards Association (VESA), Society of Motion, Picture and Television Engineers (SMPTE), ITU, Info Comm and Information framework (SID) that have made been involved in the standardisation process or made announcements on VR, AR, MR standards. Internationally, as well, the proliferation of these standards is limited.

Consumer IoT: Consumer IoT products are likely to see significant outreach in the next few years in India. At least 9.5 percent of Indian homes are expected to be outfitted with smart devices by the end of 2023. Our case studies highlight that consumer IoT solutions currently lack standards for handling unstructured data and ensuring security. Current communication and interconnection standards and regulations are inadequate to address data interfacing requirements. Open Connectivity Foundation will provide the first international smart home standard to ensure robust and secure connectivity by completion of OCF 2.1 certification. The OCF India chapter was launched on May 10th, 2019. Samsung Research and Development Institute in partnership with Nasscom, Intel and L&T announced the formation of the OCF India Ecosystem Task Force to increase awareness about global Internet of Things (IoT) standards and its benefits for the Indian IoT Industry. Since India is vulnerable to IoT attacks, product development

5 Hoppe. S (2017). There Is No Industry 4.0 without OPC UA, Automation.com https://www.automation.com/automation-news/article/there-is-no-industry-40-without-opc-ua

must prioritise security of devices. Security is one of the primary reasons for the slow adoption of consumer IoT in India.

Smart Cities: The Smart Cities Mission in India aims to promote sustainable and inclusive development of cities. Each of the core infrastructure components involves the use of technology, information and data to improve the quality of services. At present ISO, IEC and ITU are the three main international bodies that qualify as standards bodies for smart cities. Besides the three international steering bodies, standards for smart cities, including for smart grids, smart metering, 3D video standards, smart vehicles, etc. are also being developed by IEEE, to enable consumer connectivity. In India, the Bureau of India Standards (BIS) and the Telecommunications Standards Development Society India (TSDSI) have formed dedicated working groups for standards on M2M, IoT and Smart Infrastructure. These efforts are yet to see fruition, as proposals in the pre-standardisation study are still to be formally accepted by the concerned departments. ETSI and TSDSI, both oneM2M partners are collaborating on a series of standardisation subjects, especially in the domain of M2M and IoT. The use of oneM2M is slowly gaining popularity. HP's oneM2M platform has also been selected by the Bhopal Smart City Development Corporation Limited to created India's first cloud-based and integrated command and control center. Since, HP has deployed its oneM2M platform across seven cities in MP. According to industry sources, the efficiencies of oneM2M kick in for a project with minimum 20000 devices. However, in case of smaller and less complex installation, onem2M may become an overkill, given the costs associated with implementation of oneM2M. Accordingly, technology companies may use alternate platforms such as Trinity and Fluentgrid for aggregation and exchange of data in IoT system. The challenge with smart buildings and smart cities is the availability of affordable harmonized standards. Consensus building among stakeholders in the IoT ecosystem is a key requirement to speed up the standardisation process for smart cities. Moreover, the ecosystem must be dynamic to enable modifications and upgradations to current standards.

India is a latecomer to standard setting for IoT. U.S, Germany, Japan and Russia have enjoyed first mover advantages in standard setting. Setting up of TSDSI was a significant milestone for India. It created an ecosystem that works towards developing and promoting India–specific requirements for IoT. Government must step up its role in facilitating the development and adoption of standards. India needs to put efforts both in standards development and adoption. Some of our specific recommendations include

- **Encourage Centralised and Co-ordinated Development**: The multitude of IoT verticals leads to the creation of silos which precludes the congregation of rich data sets collected by vendors of each vertical and can sometimes lead to a duplication of standardisation work amongst different SDOs. If collaboration isn't pursued as a value-goal, it defeats the inherent purpose of deploying IoT. A coordinating agency must be designated the task of harmonizing the standardisation needs across various verticals and simultaneously work on strengthening the horizontal platform.

- **Strengthen Governance of Indian Standards Bodies:** An assessment of the functioning and governance mechanisms including membership fees, policies, norms, guidelines and good practices, policies on IPRs etc. of various SDOs in India would be a good starting point to check against anti-competitive outcomes and achieve objectives of maximum participation, speed of standard adoption, etc.

- **Invest in Research and Development**: The importance of research and innovation cannot be overstated for development of standards. India can work with a middle path that enables the private sector as well as supports key government-led development initiatives. The government must focus on building skill sets necessary for IoT research. This implies strengthening the educational curriculum around IoT including certification courses, exchange programs, trainings, etc.

- **Integrate MSMEs and Start-ups:** Both standards development and adoption are expensive propositions and MSMEs as well as start-ups need to be hand-led both technologically as well as financially to encourage adoption of new standards. This triple helix approach, popular in many countries can become the way forward for India.

- **Enhance Participation in Global Platforms**: A unanimous response from stakeholders suggests that India's biggest disadvantage is its underrepresentation in global standards fora including ITU-R, 3GPP, One M2M, ITU-T etc. TSDSI has made specific recommendations on improving the participation of India in global fora. This includes creating a pool of standardisation experts, bringing more global platforms to India, enhancing influence through local and regional alignments.

- **Build Awareness among the Developer Communities:** At present the stakeholders including academia, industry, start-ups etc. lack awareness on the standards and the standard development process. Organising hackathons is a good way to create awareness among developers and encourage them to develop utilities, ideas, sample code and solutions using standards.

- **Encourage IoT Consultancy and Certification Services:** The multiplicity of products and standards can lead to a choice paralysis for end users (such as vendors and different corporations) and may result in sub-optimal choices led by cheaper but poorer technologies. India can consider adopting the BSI's (British Standards Institute) testing and certification for connected IoT devices helps new manufacturers gain market acceptance.

- **Focus on Standards for Smart Cities:** At present, there is limited interoperability in the smart cities ecosystem that is locked in by bigger vendors. The technology trends in "Smart Homes", "Smart Building", "Smart Grid", "Smart Water", "Smart Transport" and "Smart Cities" are deployed in silos leading to inefficiencies. There is need for a common framework and defined architecture for the software, hardware and network infrastructure to be deployed. Since data is crucial for smart cities, a comprehensive data management standard in India will enable quick scaling and also instil public confidence and trust. Standards National Action Plan (SNAP) 2019 from BIS seeks to mitigate this problem by facilitating the creation of standardisation cells. However, we must guard against the general lack of coordination on an inter-ministerial level as well the centre and other private entities. As of 24th June, 2020, no standardisation cells are visible on the BIS website.

- **Focus on Standards for Cyber-Security Governance:** The present IoT policy encourages public-private partnerships (PPP) to secure critical infrastructure in the IoT domains. However, the implementation is not full proof. The government's top down approach is hindering coordination and cooperation between various parties. The Indian IoT solutions especially IIoT is in dire need of a standard to reduce security risks which currently lacks implementable reference architecture. The lack of trust in devices is limiting the adoption of Consumer IoT. A key focus area for IoT standards in India should be securing the ecosystem and all interconnected devices.

1. Introduction

The idea of connected devices, often called the "embedded internet[6]" or "pervasive computing" has been prevalent since the1970s. In 1999, the phrase "Internet of Things (IoT), was first used by Kevin Ashton (co-founder and executive director of the Auto ID Center at MIT) for his presentation on concatenating radio-frequency identification (RFID) technology to the Internet, the zeitgeist of the time[7]. Since then, the connotation of the phrase has been in a constant state of flux, and a wide array of definitions has emerged.[8]Over time its progression and application into numerous technologies like wireless networks, micro electromechanical systems (MEMS), micro services, embedded systems and sensors[9]has made it cumbersome and difficult to arrive at a comprehensive definition for IoT. While there is no unanimous consensus on what 'exactly' constitutes IoT[10], it can be broadly defined as "the networked interconnection of everyday objects, which are equipped with ubiquitous intelligence". Alternatively, it is also defined as a group of "interconnected objects that are identifiable and equipped with sensing, computing, and communication capabilities"[11].Several standard developing organisations (SDOs)/ standard setting organisations (SSOs) have also published their own definitions of IoT.

According to a white paper released by Cisco's Internet Business Solutions Group (IBSG), the conceptualization of IoT can be dated to 2008 - 09.[12] This was simply based on looking at the time period during which the number of connected "things or objects" exceeded the number of humans connected to the internet. IoT started to gain traction in 2010, when an audit of Germany's data protection authority found Google Street View to be 'accidentally' storing payload information from open Wi-Fi[13]. In the same year, China's National Economic and Social Development Plan itemized IoT as a strategic priority for the next five years.[14] In 2011, IoT was added to Gartner's annual hype cycle for emerging technologies.[15]

United States and China are currently leading the global race in IoT development, collectively spending USD 376 billion on IoT-led innovations. They are followed by Japan ($65.4 billion), Germany ($35.5 billion), Korea ($25.7 billion), France ($25.6 billion), and the United Kingdom ($25.5 billion)[16]. According

6 This term was first used in 1974 and describes a computer that is physically incorporated into a larger system whose primary function is not data processing, and integral to such a system from a design, procurement and operations viewpoint. Manley J.H. AFIPS '74 Proceedings of the May 6-10, 1974, National Computer Conference and Exposition. ACM Press; New York, NY, USA: 1974. Embedded Computers: Software Cost Considerations; pp. 343–347. [CrossRef] [Google Scholar] [Ref list]

7 Ashton. K (2009) "That 'Internet of Things' Thing, RFID Journal. https://www.rfidjournal.com/articles/pdf?4986

8 Ibid. In 2009, Ashton envisioned that the central tenet of IoT was to empower 'things' to accurately gather and process data while simultaneously decreasing the dependence of canonical systems and architectures on people to do the same

9 Wigmore I. (2014). "Internet of Things (IoT)", *TechTarget,* 28 July 2019.

10 Meddeb. A (2016). Internet of things standards: who stands out from the crowd?", IEEE Communication Magazine, Volume 54, Issue 7, July 2016. Page 40-47

11 Tandon, P. (2016). Internet of Things: The next evolutionary step- A Review. *International Journal of Students' Research in Technology & Management*, *4*(2), 30-34. Retrieved from http://giapjournals.com/index.php/ijsrtm/article/view/ijsrtm.2016.422

12 Evans, Dave. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. Cisco Internet Business Solutions Group (IBSG), 2011, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.*

13 Kiss. J (2010). Google admits collecting Wi-Fi data through Street View cars", *The Guardian*, 15 May 2010.

14 Report on the Implementation of The 2010 Plan for National Economic and Social Development and On The 2011 Draft Plan for National Economic and social development Fourth Session of the Eleventh National People's Congress March 5,2011 National Development and Reform Commission

15 "Gartner Hype Cycle: Internet of Things Makes the List." *Posts capes*, https://www.postscapes.com/internet-of-things-added-to-the-2011-hype-cycle/.

16 IDC. https://www.idc.com/getdoc.jsp?containerId=prUS44596319

to the latest forecast by International Data Corporation (IDC), the Asia Pacific region {China ($168.6 billion), South Korea ($26.2 billion) and India ($20.6 billion)} is expected to become the leader in global IoT spending.[17] COVID-19 is estimated to push out the growth of global IoT markets from USD 150 billion in 2019 to USD 243 billion by 2021. A large part of this growth is likely to come from the Asia Pacific[18].

The explosive growth in mobile devices and the increasing ubiquity of wireless connectivity has propelled the growth of IoT and its applications across several countries. Remote health monitoring, disease detection and monitoring, crop monitoring, accident prediction and detection, traffic monitoring, robotic rescue operations and environmental pollution monitoring are some of the common IoT applications that we witness today[19]. In 2018, The productivity gains from IoT in United States and China was estimated to be more than 50 percent[20]. While whole new business models are being developed around the IoT product line, traditional businesses are also deriving benefits from the technology by using it to deliver new products, provide customization, reduce operating costs and enhance overall efficiency.

One of the most structured applications of IoT across countries is Smart Cities. The use of IoT in governance is making urban life attractive by providing intelligent transportation systems, energy efficient buildings, waste management systems, etc. With an increasing number of applications and devices, global IoT spending is expected to touch $1 trillion by 2023[21].[22] Discrete manufacturing, process manufacturing and transportation are expected to be the three commercial industries spending most on IoT solutions in the near future[23].

The installed base in the consumer sector is forecasted to be 12.86 billion by 2020, 14 percent of which will come from the automobile sector[24].Within the industrial sector, low cost and high-volume cross-industry devices, such as those targeted at smart buildings (including LED lighting, HVAC and physical security systems) are expected to take lead. However, applications tailored to specific industry verticals (including manufacturing field devices, process sensors for electrical generating plants and real-time location devices for healthcare)are projected to grow from 1.63 billion units in 2017 to 3.17 billion in 2020, attaining a 24.57% compounded annual growth rate (CAGR) in three years[25]. *Figure 1.1* below provides a summary of IoT trends worldwide. The continuing decline in the cost of sensors will also drive the proliferation of IoT applications[26]in the future. A sensor that costs USD 0.5 today is expected to be available for USD 0.34 soon[27]. IoT possesses the potential to transform the fundamental structures and functioning of businesses and societies. The productivity gains from IoT are expected to be over USD 370 billion per annum in 2025[28].

---

17 *ibid*

18 https://www.marketsandmarkets.com/Market-Reports/covid-19-impact-on-iot-market-212332561.html

19 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

20 *Ibid*

21 IoT News (2019). "Global IoT spending to break $1 trillion by 2023 – fuelled by solid consumer and commercial adoption", June 14, 2019. https://www.iottechnews.com/news/2019/jun/14/global-iot-spending-break-1-trillion-2023-fuelled-solid-consumer-and-commercial-adoption/

22 State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. IoT Analytics. August 8, 2018.

23 *Ibid*, Footnote 10

24 Statista

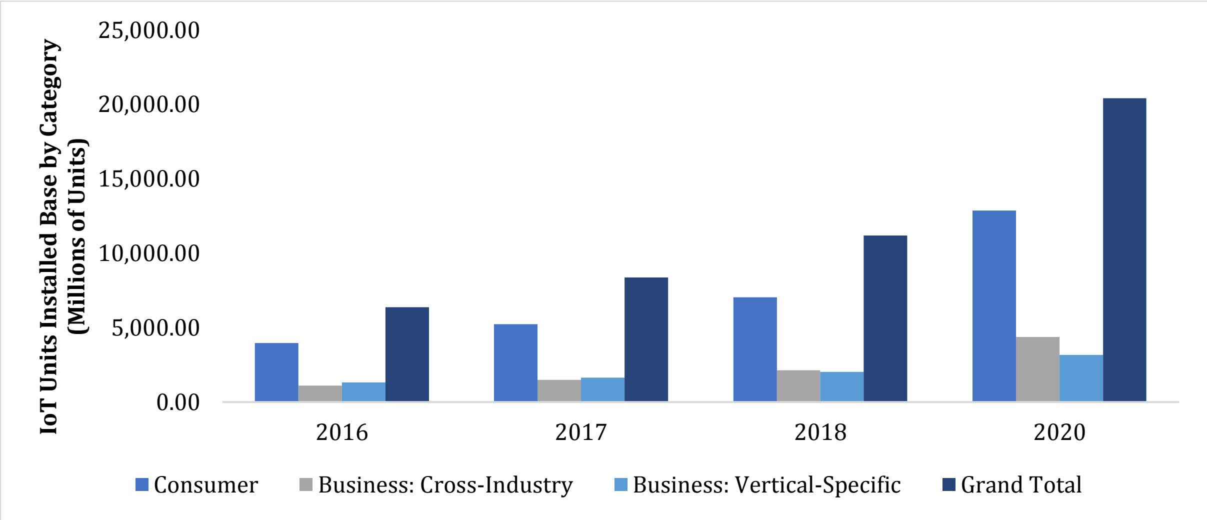
25 *Ibid*

26 https://www.theatlas.com/charts/BJsmCFAl

27 Deloitte Analysis, Industry Reports

28 Sivakumaran. M and Castells. P (2019). "The contribution of IoT to economic growth Modelling the impact on business productivity", GSMA Intelligence, April 2019.

Figure 1.1: IoT Units Installed Base by Category (Millions of Units – Actual and Projected)



Source: Gartner (January 2017)

India's digital ecosystem provides several opportunities for IoT to grow and thrive. The IoT market in India was estimated to be USD 1.3 billion in 2017 and is likely to expand to USD 9 billion by 2020[29], with an installed base of 1.9 billion units. Utilities, manufacturing, transport and logistics together account for nearly 60 per cent of industrial IoT in India[30]. The interplay of existing software, telecom and electronic hardware capabilities will facilitate growth of IoT in the future. Government policies are cited as the major catalysts in this process.[31]The IoT policy document published by the Ministry of Electronics and Information Technology (MEITY) in 2016, sets out a vision to "*develop a connected and smart IoT based system for India's economic, societal and environmental needs*"[32].India's Smart City Mission focuses on the use of IoT based smart solutions to improve land use, create walk able societies, promote transportation options, preserve and develop open spaces, etc.[33]. Policies under the Digital India Program also discuss the wide scale deployment of IoT solutions for Industrial IoT applications[34].While Industrial IoT is predicted to grow at a relatively expedited rate, the current cost of IoT devices coupled with security and privacy concerns will inhibit the immediate growth of consumer IoT devices in the country. A collaborative report by IAMAI (The Internet and Mobile Association of India) and Deloitte also forecasts Industrial IoT to supersede the Indian consumer IoT market space by as early as 2020.[35]

However, for market forecasts to manifest into an economic reality, smooth standardisation of products and processes is critical. The past decade has overseen the emergence of a fragmented and proprietary IoT

---

29 Deloitte Analysis, NASSCOM https://www.wfeo.org/wp-content/uploads/stc-information/L3-IoT_Landscape-by-S_Malhotra.pdf

30 *Ibid*

31 Priya (2019). Future of IoT in India – Current Market Trends and Use Cases, Wire 19. https://wire19.com/future-of-iot-in-india-current-market-trends-and-use-cases/

32 IOT Policy Document https://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20%281%29.pdf

33 Smart City Mission : http://smartcities.gov.in/content/innerpage/smart-city-features.php

34 Draft Policy on Internet of Things, Department of Electronics & Information Technology(DeitY) Ministry of Communication and Information Technology Government of India

35 Priya (2019). Future of IoT in India – Current Market Trends and Use Cases, Wire 19. https://wire19.com/future-of-iot-in-india-current-market-trends-and-use-cases/

ecosphere[36], with most companies trying to create niche markets and promote their own 'Internet of Things[37]'.An environment of vendor lock-ins tends to subvert the basic principle of interoperability which lies at the core of IoT solutions. Standardisation is essential for the deployment of IoT as it enables interoperability, security, privacy and provides plug and play opportunities for new solutions in the market. While standardisation is critical, its economic consequences are not straightforward. Standards facilitate structured innovation[38] and the entry of new products conforming to them, thereby enabling network externalities and healthy competition in the market. At the same time, standards can also confer monopoly power to companies developing the standard. According to European Union Agency for Cyber security (ENISA's) Security Standards Gap Analysis[39], standards have two main functions a) ensuring interoperability and b) promoting confidence. While the literature on interoperability is significantly mature, discussions on promotion of confidence has begun to gain traction in the wake of recent high-profile privacy scandals, with trust, security and privacy now forming key pivots to ubiquitous IoT proliferation[40].

Given this background, the objective of the report is to

- Outline and compare the standard setting process across different standard setting organisations that contribute to the service, application, communication and device layers of the IoT ecosystem.
- Examine the role of all stakeholders in the standard setting process by evaluating the governance framework for standard setting organisations (SSOs)
- Outline case studies that provide a comparative understanding of the role of standards and SSOs in the IoT ecosphere.
- Scope the global standardization precedents and present a comparison of IoT policies across different countries
- Provide policy recommendations to accelerate standardisation of the IoT Ecosystem in India

2. Literature Review

Standardisation as defined by the International Organization for Standardisation (ISO) and the International Electro technical Commission of standardisation (IEC) is a "*common and repeated use of rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context*[41]." There is however a precedent where an industry convention has indirectly impeded a supposedly superior technological alternative from scaling, thereby precluding their assumption of a de jure status i.e. legally recognized by law. The QWERTY keyboard is an example of such an instance[42]. Invented by

36 Darmois. S, Daniele. L, Guillemin. P, Heiles. J, Moretto. P and Van der Wees. A: IoT Standards Landscape – State of the Art Analysis and Evolution. https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609105C6.pdf

37 Basulto. D (2015). 3 reasons why the Internet of Things (still) doesn't make sense, The Washington Post.

38 Blind, Knut. The Impact of Standardization and Standards on Innovation. Manchester Institute of Innovation Research, 2013, The Impact of Standardization and Standards on Innovation.

39 IoT Security Standards Gap Analysis v1.0 | December 2018

40 Meddeb. A (2016). Internet of things standards: who stands out from the crowd?, IEEE Communications Magazine (Volume: 54 , Issue: 7 , July 2016)

41 Blind. K (2013). "The Impact of Standardization and Standards on Innovation", Nesta Working Paper 13/15 November 2013 www.nesta.org.uk/wp13-15. https://media.nesta.org.uk/documents/the_impact_of_standardization_and_standards_on_innovation.pdf

42 Allen. R and Sriram R (2000). "The Role of Standards in Innovation", Technological forecasting and social change , 64, 171-181 (2000), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=821473

Christopher Latham Sholes in 1867[43], the arrangement of the keys was predicated on the frequency of use of letters in the English alphabet. It was created in consultation with many typists to determine the best placement of alphabets on a keyboard that would result in fast typing with both hands and prevent jamming in old mechanical typewriters. Jamming became obsolete with the advent of the personal computer. QWERTY rapidly gained traction and was adopted by manufacturers on a large scale[44]. However, "better" (the term better here entails user subjectivities due to certain constraints in experimental results[45]) keyboards were developed over time. A popular one was developed by August Dvorak that increased the typing speed by 20 percent and reduced the movement of hand speeds by 1/16th in comparison to QWERTY keyboard. However, the ubiquity of the QWERTY keyboard (thus implicitly indicating its assumption of a de facto status) across various industries coupled with human inertia to change to new alternatives (the power of default as discussed by Richard Thaler) precluded the rise of other alternatives liked VORAK[46]. Thus, QWERTY still retains its status as the most pervasive keyboard across the globe.

The example highlights the sticky nature of some standards. One can now argue that stickiness doesn't always imply technical superiority. The example of Betamax and Video Home Systems (VHS -formats of videotape technology during the late twentieth century) succors in that pursuit. Betamax was developed by Sony while VHS was developed by the Victor Company of Japan (popularly known as JVC). Both these standards of videotape formats were incompatible[47] with each other and led to a divided market with both companies competing for relative dominance. After years of competition, VHS turned out to be the winner in the videotape war, even though Betamax was found to be technologically superior. While an optimistic analysis of the above situation might highlight the ability of market forces to evaluate standards through a multi-faceted lens rather than a purely technological dimension, a pessimistic point of view highlights the potential of standardisation to create vendor (industry) lock-ins. The case of Qualcomm (which holds numerous patents for wireless modems) is another example.[48]The company was accused of unfair treatment to phone makers by charging disproportionately high royalties or refusing to license essential patents. The Federal Trade Commission sued the company for having "harmed competition in two markets for baseband processors.

Numerous examples of innovation, including those in railroads, modern manufacturing, agriculture and logistics, would not have succeeded in the absence of standardisation. Studies conducted by ISO conclude that companies achieve tangible benefits by applying standards. They can streamline operations, improve financial returns and provide opportunities to enter new markets[49]. In addition, standards also build credibility for new technologies and products by reducing risks for users.

---

43 Ash win (2015). "Evolution of Keyboards: Why Is Qwerty the Most Preferred Keyboard?", Science ABC. https://www.scienceabc.com/innovation/qwerty-keyboard-over-the-years-why-is-it-the-most-preferred-typing-tool.html

44 Dedhia. Z (2014). "The Secret History of Keyboards (QWERTY vs DVORAK)", TechTricks World, August 24, 2014. https://www.techtricksworld.com/secret-history-keyboards-qwerty-vs-dvorak/

45 Though experimental results highlighted that DVORAK keyboards lead to faster typing speeds, it becomes to cardinal to also realize that the users of the experiment were trained to type on DVORAK keyboards. In the light of this premise, some could argue that the results were skewed. One can also point out the lack of rigorous studies that juxtapose the speeds of the two keyboards in a fairly objective manner.

46 *Ibid*38

47 Essays, UK. (November 2018). The Lock in Effect and Its Causes. Retrieved from https://www.ukessays.com/essays/economics/the-lock-in-effect-and-its-causes-economics-essay.php?vref=1

48 Robertson. A (2019). "Competitors say Qualcomm is running a monopoly — here's why", The Verge, January 9, 2019. https://www.theverge.com/2019/1/9/18173756/qualcomm-ftc-antitrust-monopoly-trial-explainer

49 Gerundino. D, Weissinger. R , Grosfort. J and Diamond. X (2014). "Economic Benefits of Standards, International Standards Organisation (ISO), https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/ebs_case_studies_factsheets.pdf

The complex and dynamic nature of Internet of Things (IoT) can make standardisation a challenging task for the industry. The design architecture comprises of different layers which must comply with fundamental issues of inter-operability, security, scalability and network feasibility. In the absence of standards, we run a risk of technologies not serving their intended purpose with shorter lifespans[50]. The three key advantages of standardisation for IoT include (i) scalability, (ii) security and reliability and (iii) inter-operability. These are discussed below.

- ***Scalability***

Standards provide guidelines and recommendations on the use of different components and protocols in a product or a service[51]. This offsets fragmentation in productions of goods and services. It provides a skeletal structure to innovation and a uniform archetype upon which businesses can then develop new technologies and enhance existing practices. This uniformity helps decrease capital and operational costs of firms to a great extent, thus securing scalability. IoT standardisation can help industry scale and develop cutting-edge applications.

- ***Security and Reliability***

The use of packet-switched networks (PSN) make connected devices in an IoT ecosystem vulnerable to cyber-attacks. A Hewlett Packard study found that 70% of the common smart home devices were susceptible to cyber-attacks and each device had an average of 25 vulnerabilities[52]. Moreover, these vulnerabilities were rudimentary in nature highlighting the security standard gaps in the product development process. The most prominent example is that of Botnets. Botnets[53] are used by criminals for stealing private information, exploiting online-banking data, initiating distributed denial of service (DDoS)-attacks or for spam and phishing emails[54]. In the IoT ecosphere, the Mirai Botnet (ideated by Paras Jha for a frivolous end[55]) underlined the dangerous potentiality of such attacks[56]. A technical survey performed by privacyrights.com on 43 healthcare mobile applications found that only 15% apps encrypted all the data transmitted[57]. Furthermore, none of the apps encrypted data that was stored on the user's device. Development of security standards for IoT has become a necessity and is fundamentally linked to the ability of users to trust their digital environment.[58]

---

50 Jibran Saleem, Mohammad Hammoudeh, Umar Raza, Bamidele Adebisi, and Ruth Ande. 2018. IoT Standardisation - Challenges, Perspectives and Solution. In Proceedings of ICFNDS' 18, Amman, Jordan, June 26-27, 2018, 9 pages. DOI: hŠps://doi.org/10.1145/3231053.3231103

51 IoT Standardisation: Perspectives, Challenges and Solutions by Jibran Saleem

52 Rawlinson. K (2014) "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", HP, July 29, 2014. https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

53 A network of systems combined together with the purpose of remotely taking control and distributing malware

54 The Mirai Botnet hacked into some Internet of Things devices — in this case mainly routers and Internet Protocol (IP) cameras — and transformed the devices into botnets. The centrally-controlled IoT botnets flooded Dyn's, a Domain Name Services (DNS) provider, traffic causing a disruptive bottleneck that blocked Internet access for millions of users worldwide.https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

55 *Ibid*

56 Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 2017.

57 Ackerman. L (2013). Mobile Health and Fitness Applications and Information Privacy Report to California Consumer Protection Foundation, July 15. 2013.

58 Compiled from IoT Standardisation: The Road Ahead by Arpan Pal et. al; IoT Standardisation: Challenges, Perspectives and Solutions by Jibran Saleem et. al; IoT and Security Standards and Best Practices (Cisco Press) by Rik Irons-Mclean et. al; The Impact of Standardisation and Standards on Innovation by Knut Blind

- ***Interoperability***

Since the internet predates IoT, most existing standards were conceived without envisioning the scale of IoT[59]. The presence of heterogeneous sensor systems coupled with a defined set of communications and processing interfaces makes interoperability of applications and devices cumbersome. In 2015, a report by McKinsey& Company concluded that incompatibility was the number one problem facing IoT growth[60]. Standardisation ensures that IoT devices conform to certain de facto protocols and processes that allow seamless connectivity with devices using different technologies. This minimises vendor lock-ins and generates spill over benefits for all stakeholders. Interoperability also drives innovation and efficiencies for IoT device manufacturers, increasing the overall value of the market[61].

There have been some attempts in the industry, for example, Apple's HomeKit, to integrate IoT devices from different manufacturers into one single user interface[62]. Similarly, Samsung's SmartThings Hub also provides functionality that is identical to Apple's HomeKit; however, both popular platforms are constrained by the limited list of compatible devices. There have been some tangible efforts to expand the coverage of that list which may be deemed as praiseworthy by many, but it doesn't address the larger problem of a fragmented ecosystem. The realization of interoperability is challenging due to two factors: a) the myriad standardisation bodies that pursue discrete endeavors (though that has reduced to an extent) b) Companies promoting their proprietary standards (precedents have been set over time[63]). Multiple standards and protocols may complicate entry for a prospective IoT vendor. The vendor's selected combination from the set of multiple standards available may not achieve the desired objectives and can in fact be counterproductive. For example, it is possible to deliver a device that can authenticate its user, encrypt the data it transmits and decrypt the data it receives, verify protocols and integrity, but still be insecure. This is primarily because the combination of standards might have gaps which weren't known to both the vendors and the SDOs[64]. A local nodal standards agency can guide vendors to avoid such mishaps. The process of developing standards should be holistic, encompassing and addressing all gaps and untoward eventualities (an exhaustive list is unrealistic and idealistic). The section below lists out stakeholders involved in developing standards across international, regional and national bodies and evaluates the governance mechanism of the SSOs.

The study has employed desk-based research which is complemented by stakeholder consultations including standard development bodies, IoT companies, startups, industry stakeholders and sector experts. Data is collected and analysed wherever possible to support our arguments. A detailed open-ended questionnaire highlighting each issue is used for interaction with all relevant stakeholders. These experiences have helped in identifying successes and failures of the existing system. As a part of the research, historical data on standards is analyzed to evaluate consequent outcomes of governing mechanisms in the standard setting ecosystem. A comparative analysis of global practices helped provide direction to the inadequacies in the Indian ecosystem and assisted in formulating policies on standards that ensure industry conformity

---

59 Pal. A, Rath. H , Shailendra . S and Bhattacharyya. A (2018). "IoT Standardization: The Road Ahead" Submitted: September 30th 2017Reviewed: February 9th 2018Published: March 29th 2018 DOI: 10.5772/intechopen.75137

60 Manyika. J, Woetzel. J ,Dobbs. R , Bisson. P , Bughin. J and Aharon. D (2015). Unlocking the potential of the Internet of Things, McKinsey Global Institute, June 2015.

61 Rose. K, Eldridge. S and Chapin. L (2015). "THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World", Internet Society.

62 Noura. M (2018). Interoperability in Internet of Things: Taxonomies and Open Challenges, Mobile Networks and Applications, 2019, Volume 24, Number 3, Page 796

63 Schneier.B (2015). "How the Internet of Things Limits Consumer Choice", The Atlantic. December 24, 2015. https://www.theatlantic.com/technology/archive/2015/12/internet-of-things-philips-hue-lightbulbs/421884/

64 Note the use of SDOs/ SSOs are interchangeable in this paper

and diffusion of the emerging technology. Use cases of IoT is documented to evaluate the scope of sectoral tailoring. Secondary data on existing standards, domestic capabilities and international collaborations is presented using descriptive statistics as can be seen in the section below.

3. Analysis and Interpretation

3.1 Standardisation Efforts: A snapshot of Global Standards Setting Organisations

Several standard development organisations (SDOs), industry consortia and alliances, across the world, are working on standards for deployment of IoT.[65]These organizations produce standards using a consensus-based transparent process. The standards are either adopted as legal requirements or left to industry as guidelines for voluntary adoption.

Standards bodies work across various IoT applications and design architectures to ensure that the deployment is interoperable and secure. Over a hundred different bodies are currently involved in developing standards across verticals such as home/ buildings, manufacturing/ industry automation, healthcare, energy, etc. as well as horizontal service and infrastructure requirements. *Figure 3.1* borrowed from *Alliance for Internet of Things (AIOTI) WG3 -Release 2.9* reflects this diversity in participation alongside a focus on niche areas. For example, the Thread Group is focused on connected homes, Apple's Health Kit works on health and fitness, EnOcean Alliance on building automation, Open Automotive Alliance on connected cars and HART Communication Foundation on industrial IoT solutions. Organisations often produce more than one standard. IEEE has published 80 standards that are applicable to IoT and an additional 45 which are under development.[66] These standard setting organisations, which can operate both in specific verticals, across verticals as well as in the horizontal layer, help consolidate an otherwise fragmented marketplace and help businesses enter an industry with a degree of certainty. It also helps companies achieve economies of scale, making solutions affordable in the long run.

Figure 3.1: IoT SDOs and Alliances Landscapes (Vertical and Horizontal Domains)

[65] Each member remains independent in normal business operations, with no say over other members' work that is not related to the consortium.

[66] http://standards.ieee.org/innovate/iot/stds.html

In a paper titled IoT Standardisation: The Road Ahead[67], SDOs have been categorized into two types: *a) Generic and b) Application specific.* The first class of SDOs has tried addressing problems for the entire ecosphere by developing technological standards and reference architectures. Organisations like ISO/IEC JTC-1 (International Organization of Standardisation and International Electro Technical Commission), ITU (International Telecommunication Union), IEEE (Institute of Electric and Electronic Engineers), IETF (Internet Engineering Task Force), 3GPP (3rd Generation Partnership Project) and oneM2M fall under this category. The second class of SDOs focuses on standardizing technology for a specific domain of applications. Their activities try addressing gaps in already available standards offerings. For instance, Fairhair Alliance[68]led by companies from the lighting, building automation, semiconductor and IT industries develops IoT applications for commercial buildings. Other standards organisations such as Hypercat[69], IoT security foundation[70], wireless IoT forum[71], etc. also work on specific domains and have been involved in the discussion on IoT standards. Some standards organisations on IoT such as IoTivity[72], AllJoyn[73], OPENIoT[74], etc. can be grouped into a category of open source initiatives which provide flexibility to customize verticals of the IoT ecosystem. The details on the scope and objectives of the various SDOs and alliances involved in developing standards for IoT is provided in *Appendix 1*.

While mainstream SDOs and alliances are actively working on IoT services and architectures, many independent and state-funded projects are also being carried out to support and promote IoT. Countries including India, China, Korea, Japan, Europe and the USA adapt global recommendations to suit local requirements of IoT deployment. The section below provides a detailed analysis of the various standardisation efforts taken by India to harness the IoT potential.

3.1.1 Standardisation efforts in India

Since 1947, the standardization efforts in India have been led by the Bureau of Indian Standards (BIS). Additionally, more than 25 other bodies which include ministries, regulatory bodies, public sector

---

67 Pal. A, Rath. H, Shailendra . S and Bhattacharyya. A (2018). "IoT Standardization: The Road Ahead"Submitted: September 30th 2017Reviewed: February 9th 2018Published: March 29th 2018 DOI: 10.5772/intechopen.75137

68 https://www.fairhair-alliance.org/about-fairhair/what-is-fairhair.html

69 Hypercat is a consortium of global hardware and software vendors that is driving the Hypercat standard. The Hypercat standard is an open, lightweight JSON-based hypermedia catalog format for exposing information about IoT assets over the web. The aim of Hypercat is to help unlock the full potential of IoT by breaking down data silos, and providing an automated way of discovering services and getting access to them. The Hypercat Alliance strives to be a one-stop shop of best practices for IoT implementations. Its advisory board consists of Cisco, Symantec, WSP, BT and KPMG. These companies are building Hypercat into the work they are doing in the IoT smart city and manufacturing settings. Hypercat is being used in the CityVerve smart city project in Manchester as a way to build security into the project from the ground up

70 An industry association comprising over 50 members (including ARM, BT, Vodafone and various universities) that aims to promote best practice and knowledge sharing in IoT security

71 An industry body that is aiming to drive consensus and interoperability in low-power, wide-area (LPWA) wireless communication standards for the IoT, including both standards using unlicensed and licensed spectrum. It is not strictly a standards body but aims to promote appropriate solutions to the relevant standards bodies

72 IoTivity is an Open Source Project sponsored by the Open Connectivity Foundation (OCF) / OIC and hosted by the Linux Foundation. The aim of this project is to develop an open source software framework to seamlessly connect the billions of devices in the emerging Internet of Things (IoT), across multiple operating systems and network protocols.

73 AllJoyn is an open source software framework that makes it easy for devices and apps to discover and communicate with each other.In October 2016, the AllSeen Alliance who sponsored the AllJoyn Project, and the Open Connectivity Foundation (OCF) merged. One result of the merger was the creation of the OCF Resource to AllJoyn Interface Mapping specification to assist vendors migrating from AllJoyn to OCF.

74 OpenIoT is a joint effort of prominent open source contributors towards enabling a new range of open large scale intelligent IoT (Internet-of- things) applications according to a utility cloud computing delivery model.

undertakings, technical development agencies, commodity boards etc. are involved in sector specific standardisation work[75],having developed 20,488 Indian standards mostly in the product segment and support standards such as test methods, terminology, codes of practice, etc.[76]Of this, 7,267 are unclassified standards. Many foreign organizations are also facilitating standard adoption in India. These efforts have led to harmonization of several sectoral products and test methods. However, the needs of standard development, testing and adoption are limited by the availability of resources.[77]Standardisation has become critical in the light of exponential growth of IoT in India. As highlighted in the introduction, the market is expected to reach USD9 billion by 2020[78]. The applications will lie in the domain of agriculture, health, water, natural disasters, transportations, security, etc.[79]. For the ecosystem to flourish, development and harmonization of standards across all the layers would be essential.

Using the interpretation of the BIS Act of 2016, India's national SDO can be regarded as both generic as well as application specific. In practice however, it leans more towards the functions of a generic SDO. BIS publishes IoT related standards under eight different working groups of the Electronics and Information technology (LITD) technical departments a) LITD 27: Internet of Things and Related Technologies; b) LITD 28: Smart Infrastructure; c) LITD 29: Block chain and Distributed Ledger Technologies; d) LITD 30: Artificial Intelligence; e) LITD 31: Cloud Computing, IT and Data Centres; f) LITD 32: Biometrics; g) LITD 33: Wearable Electronic Devices and technologies; h) LITD 34: Smart Manufacturing Sectional Committee. Further details are provided in *appendix 2.1*

The Telecommunications Standards Development Society, India (TSDSI) is an application specific SDO within the generic SDO jurisdiction. This is because TSDSI primarily focuses on developing India specific Telecom/ICT standards. TSDSI and Telecommunications Technology Association (TTA) signed a MoU in March, 2019 to collaborate on research in IoT/M2M, AI and 5G as key focus areas[80]. TSDSI has also transposed several standards from oneM2M, the global organisation working towards the creation of a global technical standard for interoperability of IoT technologies. This has precluded duplication of standards work to a great extent as the important areas of security, interoperability and functional architecture are extensively covered under the transposed standards. Similarly, it has also transposed some essential standards from 3GPP as summarized in Appendix 2.2

The Telecom Engineering Centre (TEC) provides support and advice to DoT on technology, spectrum and licensing related issues and produces standards related documents. TEC develops telecom product specification and interoperability (interface) specification for seamless working of telecom networks and devices. These also cover safety and security requirements. The Telecom Engineering Centre (TEC) under the department of telecom (DoT) is finalising 5G standards for telecom equipment and devices. The roadmap for M2M communications was released in May 2015 but the centre is yet to finalise generic requirements for the segment. *Table 3.1* below summaries India's efforts towards standardisation of the IoT ecosystem and the role of different standards organisations.

---

75 Indian National Strategy for Standardization (2018) https://commerce.gov.in/writereaddata/uploadedfile/MOC_636552662013452841_INSS_draft_23-2-18.pdf

76 *Ibid*

77 Building a National Strategy Framework for Standardization Anupam Kaul CII.http://indiastandardsportal.org/Standards%20Conclave%202017-%20DAY%201/Session%201/Anupam%20Kaul%20%20.pdf

78 Future of IoT, FICCI. http://ficci.in/spdocument/23092/Future-of-IoT.pdf

79 https://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf

80 Vanshika (2019). TSDSI and TTA sign MoU to collaborate with focus on AI, 5G, IoT/M2M, Broadcasting, PPDR and Railway Communications, TSDSI. March 27, 2019. https://tsdsi.in/tsdsi-and-tta-sign-mou-to-collaborate-with-focus-on-ai-5g-iot-m2m-broadcasting-ppdr-and-railway-communications/

Table 3.1: Standards bodies and their initiatives on IoT standardisation in India

Standard Development Organization (SDOs)	Focus Area and Objectives
Telecommunication Standards Development Society (TSDSI)	• Founded in 2013 • Working Group 8 on M2M studies and Indian requirement for M2M and IoT solutions. • In 2015, TSDSI joined the one M2M consortium • TSDSI has transposed 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 IoT and telecommunications • TSDSI recently contributed a Low Mobility Large Cell (LMLC) standard to ITU-R – cleared STEP 3, considered for evaluation as an IMT-2020 (5G) standard
Bureau of Indian Standards (BIS)	• BIS has taken initiatives to identify India specific requirement for a unified, secure and resilient ICT backbone for smart cities. • The IoT panel focuses on IoT, big data, sensor networks. The standards are directly under development at JTC -1 • A pre-standardisation study titled "Technical Requirement Analysis of Unified, Secured and Resilient ICT Framework for Smart Infrastructure" was released in November 2017. • LITD 28 has also constituted a study group on 5G imperatives for Smart Infrastructure to define a smooth migration path from current frameworks and architectures to '5G inclusive' next generation homogeneous architectures
Telecommunication Engineering Centre (TEC)	• The Telecom Engineering Centre (TEC) under the Department of Telecom is finalising standards for telecom equipment and devices for 5G services. The roadmap for M2M communications was released in May 2015 but the centre is yet to finalise generic requirements for the segment. • Various divisions in TEC, chair the National Working Groups (NWGs) corresponding to the study group of ITU-T. TEC also chairs NWG-5 corresponding to study group 5 of ITU-R, which deals with standards for mobile radio systems. TEC runs an IPV6 Ready Logo Test Lab, Specific Absorption Rate (SAR) Lab and Next Generation Network (NGN)/ Transport Lab.

The Seconded European Standardization Expert for India (SESEI)	• SESEI launched in March 2013, is the India body for The European Telecommunications Standards Institute ("ETSI"). • It raises awareness on the European Standardisation System in India. The focus areas include M2M/IoT, security, 5G, NFS/SDN etc. • It facilitated the MoU between COAI and ETSI to promote adoption of standards-based communication technologies
The Global ICT Standardization Forum for India (GISFI)	• An Indian standardisation 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.
IoT for Smart Cities Task Force (IoT4SCTF)	• The forum is funded by MEITY and has recently released the draft IoT framework for the reference architecture of smart cities
India –EU Cooperation on ICT related Standardization Policy and Legislation	• The overall objective of the project "India-EU Cooperation on ICT-Related Standardisation, Policy and Legislation" (2015 – 2019) is to promote closer alignment between India and Europe • They are making provisions for technical assistance in the identified priority fields 5G, NFV/SDN, Intelligent Transport Systems (ITS), and Security. This includes position papers and analyses/studies on specific standardisation aspects.

Source: Compiled from SDOs/ alliances websites

India's contribution to standards development however has been very limited. The ongoing efforts are also at a nascent stage and mostly driven by global companies operating in India.[81]Establishing TSDSI in 2014 was a step in the right direction; the standardisation efforts at TSDSI have seen some early success. However, any degree of maturity would require concentrated effort including active pre-standardisation dialogues that provide the platform to develop new ideas. Indian startups, consumed by challenges of viability and scalability, are unable to focus on developing and setting standards. Despite, the incubation facilitated through Centers of Excellence (CoE), most startups fail to contribute to standards development. For successful deployment of IoT, collaboration among industry, academia, global standards bodies and local SDOs are imperative. The section below outlines the functioning and governance mechanisms of various SDOs across the globe. Such assessments can be a useful guide for India to improve upon the quality of their SDOs and encourage greater participation in the domestic and global standards development process.

3.2 Participation in the Standards Development Process

Standards organisations operate in multiple formats. There is growing recognition among countries for the need to work together and establish good practices and enable broad-based participation in the standards development process. SSOs[82] encourage participation in the development process by highlighting benefits such as increasing the stakeholder's strategic and technical influence in an industry, while gaining early access to information on an evolving standard to be better placed when designing and introducing new products. Some SSOs also provide training and valuable experience to the representatives participating in the design process. They conduct seminars, produce white papers and often engage in marketing as well as technical activities. Association with SSOs also signals the member's commitment to markets, technologies or architectures. However, benefits provided by SSOs are not uniformly attractive to all types of members with an interest in standards. "Placing oneself in the standards ecosystem involves determining a number of factors, including *relationship to standards*, industry *identity*, and desired *role* in the standard setting process"[83]. Members can be either proponents or consumers of a standard; hence their choice of SSO and nature of participation may also differ[84]. While the proponent would like to reap benefits from brining standards that meet specific criteria (such as development of new markets for goods and services), consumers are largely interested in how they can employ the standards to their businesses. An antipodal yet complementary relationship thus arises. Therefore, proponents would play a more active role in a standard development organisation as compared to the consumers. The relationship to standards there for educates the attractiveness of a SSO. The identity of the participants determines their interest and objectives of participating in a standard development process. Participants can be vendors or other commercial entities, universities, colleges, governmental bodies, individuals, consumer groups and other non-profits. Their goals and degree of participation are summarised in *Table 3.2* below.

81 *Ibid*

82 SSOs/ SDOs can be used interchangeably

83 Undegrove. A. "The Essential Guide to Standards", https://www.consortiuminfo.org/essentialguide/participating1.php

84 For instance, SSO's reputation for neutrality is usually a positive to a consumer but may be a negative to a proponent that hopes to create a standard. All else being equal, as between two SSOs that could each serve as capably as the host for a new standards project, the proponent of that project will likely choose the SSO in which it enjoys the greater degree of influence.

Table 3.2: Evaluating Degree of Participation of Identities

Identity	Relationship to Standards	Degree of Influence / Participation
Vendors and other commercial entities	Proponent	largest and most economically influential category
Universities	Non-commercial proponents having professional interests in what standards are set and how they are structured Universities and colleges are standards consumers as well, and some institutions (such as most state and some private universities) are very substantial enterprises in their own right.	Limited. Academic staff participate to observe, to influence, or to discuss the development of the standards at hand, and participation would focus on those organizations that are active in disciplines of academic interest, such as computer science and geospatial information. For infrastructural staff, goals will be similar to those of other standards consumers,
Government	They are not only standards consumers and proponents, but also standards developers in their own right, through the adoption of laws and regulations that function as standards	Governments participate in SSOs at every level, from legislators and staff that liaise with SSOs, to federal agencies that are required to utilize SSO standards, to state agencies, to cities, towns and counties. When government entities participate in SSOs as consumers, they rarely join at levels that would entitle them to act on Boards of Directors or in other control functions, due to the relationship of government with the private sector.
Individual	Individuals may participate in SSOs at the behest of their employers, with the knowledge and cooperation of their employers, or independently	Limited
Consumer groups and other non-profits	Consumer	Limited Individuals are rarely interested in capacity as standards consumers, and consumer groups do not have the resources to participate in the many SSOs that do have such an impact. Non-Profit Organization has less formal liaison relationships under simple memoranda of understanding.

Source: *Undegrove. A. "Participating in Standard Setting Organizations: Value Propositions, Roles and Strategies", ConsortiumInfo.org.* *https://www.consortiuminfo.org/essentialguide/participating1.php*

The standard setting participants can therefore be categorised into three buckets (i) leaders, (ii) spectators and (iii) followers. Members categorised as *leaders* are the ones for whom participation is important to either create a new market, condition the market to demand a new product (WiFi chips and routers), service (WiMax) or computing model (service oriented architecture), or use the consortium as an extension of the members' own research and development efforts that can create high-quality technology at lower costs. While the leader can either join an existing SDO or a consortium, they sometimes form a new body to achieve their objectives even though the formation of a new consortium is costly. IBM, Hewlett-Packard, Intel and Motorola for instance have been particularly active in forming consortia, as their businesses are dependent on the predictable adoption of new standards and business models. *Followers* are members for whom participation provides a logical extension of their technical, promotional and research activities. They can technically influence, collaborate on white papers, receive advance information on the standard setting efforts and thus are able to launch new compliant products before other non-participants. Vendors and other commercial entities, governmental entities, universities and colleges are followers who can exercise their voting rights to influence the adoption of standards in the organisation. *Spectators* such as academicians and commercial entities (e.g., developers, consultants, integrators, etc.) are those for whom participation is elective. They often look for inexpensive membership to access information and knowledge on what a given consortium is doing or producing.

The leaders, followers and spectators' decisions to be associated with any standards body is also influenced by other factors including membership fees, effectiveness, speed, stability and reputation of the organisation[85]. For instance, if being a spectator is enough, then several SSOs meet the minimum standard for participation. However, if being a leader is essential, then some additional criteria become important. These include effectiveness and speed of the technical process, ease of gaining support to launch a new project and whether the SSO includes promotion as well as development of standards in its mission. The section below tries to evaluate the governance framework for some SDOs / consortia by analyzing factors such as membership fees, openness of SSOs, scope, domain, intellectual policy rights (IPR), process of ratification, etc.

3.3 Evaluation of SSOs/ Consortia

Standard Setting Organisations (SSOs) including industry and academic consortia can be distinguished across criteria such as (i) knowledge areas, (ii) membership guidelines including membership fees, (iii) norms, guidelines and good practices, (iv) ratification and (v) intellectual property rights. In the following sub-sections, we evaluate SSOs/ consortia across these different criteria. Similarly, Open source software (OSS) initiatives can also be benchmarked and compared across such criteria, discussed in *Appendix 3*. Unlike SSOs, standards that are subject to royalty or are not available for free. However, OSS is distributed with source code that may be read or modified by users as per their requirement.

3.3.1 Knowledge Areas

SSOs operating in the IoT ecosystem are spread across multiple knowledge areas. The Alliance for Internet of Things Innovation (AIOTI) 2019divided these knowledge areas into seven categories. *Table 3.3* maps SSOs across different knowledge areas which are described below.

- **Communication and Connectivity**: This includes communication protocols for wireless/ radio and wireline that generally work under the data link, network, transport[86] and application layers[87].
- **Integration and Interoperability:** Standards in these areas provide specifications for integration and interoperability of common IoT features.
- **Applications**: This area includes standards for development of the application layer such as smart homes, smart cities, etc. including development of tools, deployment standards, management etc.

[85] Ibid

[86] The transport layer provides a total end-to-end solution for reliable communications. TCP/IP relies on the transport layer to effectively control communications between two hosts

[87] The Application layer handles the interaction with the end user. All messages originate there. Commonly, the Application layer sends a string of text down to the Transport layer, which begins the encapsulation process.

- **Infrastructure**: This includes design, deployment and management of platforms that can be tailored for IoT such as software defined networks, cloud computing, mobile edge computing (MEC), fog computing, etc.[88]
- **IoT Architecture**: This comprises integrated or complete architecture specifications for IoT solutions.
- **Devices and Sensor Technology:** This covers device/sensor lifecycles, including operating systems, platforms, configuration management and sensor virtualization[89].
- **Security and Privacy**: These standards focus on security and privacy of the IoT ecosystem

88 https://aioti.eu/wp-content/uploads/2019/10/AIOTI-WG3-SDOs-Alliance-Landscape-IoT-LSP-standrad-framework-R2.9-Published.pdf

89 *Ibid*

Table 3.3: Mapping SSOs/ Consortia across Seven Knowledge Areas

IoT Alliances/ Consortia / Standard Bodies	Communication and Connectivity	Integration/ Interoperability	Applications	Infrastructure	IoT Architecture	Devices and Sensor Technology	Security and Privacy
3GPP (3rd Generation Partnership Project)							
AVNU Alliance							
The European Smart Energy Solution Provider (ESMIG)							
ETSI (European Telecommunications Standards Institute)							
Fairhair							
Global Platform							
GS1							
GSMA (GSM Association)							
Hypercat							
IEC (International Electro technical Commission)							
IEC TC57							
IEC TC65							
IEEE Standards Association							
IETF WG 6lo (IPv6 over Networks of Resource-constrained Nodes)-							
IETF WG 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e)							
IETF WG ACE (Authentication and Authorization for Constrained Environments)							
International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T)							
(ISO/IEC) JTC1/WG10 Internet of Things							

OCF (Open Connectivity Foundation)							
OneM2M							
OSGi Alliance							
TMForum							
WWRF (Wireless World Research Forum)							
UDG Alliance							

Source: *compiled from Alliance for Internet of Things Innovation (AIOTI) 2019*

Note: Cells shaded in grey indicate that the SSO/ Consortia contribute to the specific knowledge area.

From this list of prominent standard setting bodies, we find that several organisations work across different knowledge areas though they may be focusing on a select few. Moreover, organisations also evolve in their contribution to knowledge areas, and those focusing on one, may expand to related areas over a period. For example, IEEE's standardization focuses on establishing reference framework and architecture for Internet of Things. IEEE 2413 defines an architectural framework for the Internet of Things (IoT), including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety[90]. On the other hand, one M2M addresses the need for a common M2M service layer that covers requirements, architecture, API specifications, security solutions and interoperability for Machine-to-Machine and IoT technologies[91] and has been ranked as the top IoT standards body of the year. ETSI has recently released ETSI TS 103 645, a standard for cyber security in the Internet of Things, to establish a security baseline for internet-connected consumer products and provide a basis for future IoT certification schemes[92].The UDG Alliance's control and monitoring framework enables multi-protocol interoperability and integration for the Internet of Things**,** as well as large scale IoT deployment, integration and management. It encompasses over 50 communication protocols and has been used by several research projects.

Special taskforce (STF) 505 identified gaps in knowledge areas that have been considered in ETSI TR 103 376[93]. ETSI TR 103 375 assesses the degree of industry and vertical market fragmentation; and points towards actions that can increase the effectiveness of IoT standardization, to improve interoperability, and to allow for the building of IoT ecosystems. ETSI TR 103 375 [i.1] has identified a number of standards that are available, i.e. that have reached a final stage in a SDO and can be used for Large Scale IoT Pilots (LSP). The main gaps identified across knowledge areas are summarized in Table 3.4 below.

---

90 http://grouper.ieee.org/groups/2413/

91 Antipolis. S (2019). oneM2M announced as the "Top IoT Standards Body of the Year", ETSI https://www.etsi.org/newsroom/news/1582-2019-04-onem2m-announced-as-the-top-iot-standards-body-of-the-year

92 ETSI Releases First Globally Applicable Standard for Consumer Iot Security *Sophia Antipolis, 19 February 2019*

93 ETSI TR 103 376 V1.1.1 (2016-10). SmartM2M; IoT LSP use cases and standards gaps . https://aioti.eu/wp-content/uploads/2017/03/tr_103376v010101p-LSP-use-cases-and-standards-gaps.pdf

Table 3.4: STF 505 - Gaps across Knowledge Areas

Domain	Gaps
IoT Architecture	• Multiplicity of IoT HLAs, platforms and discovery mechanisms
Connectivity	• Fragmentation of the standardization landscape • Large number of heterogeneous & competing communications and networking technologies
Integration / Interoperability	• Global-level standards (international vs. regional level) • Fragmentation due to competitive platforms and standards
Device /Sensor Technology	• Quality assurance and certification • Device modularity
Service and applications	• Data interoperability: lack of easy translation mechanisms between different specific models. Need of a global and neutral data model. Seamless inter-working between data systems • Interoperable processing rules: lack of definition for advanced analysis and processing of sensor events and data to interpret the sensor data in an identical manner across heterogeneous platforms • APIs to support application portability among devices/terminals • Specific solutions at Service Layer to enable communications between the platforms (e.g., plugins to oneM2M platform)
Applications Management	• Usability [Societal gap] • Applications tailored to individual needs: evolution, flexibility of the components • Harmonized Identification • Interoperability between IoT HLAs, platforms and discovery mechanism
Security / Privacy	• Privacy and security issues can be a blocking factor for user's acceptance and prevent large scale deployments. Security and privacy are addressed on an isolated basis for part of the applications • Lack of highly secure and trusted environments • Liability for data privacy
Deployment	• Safety • Deployment tools

Source: *High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0 AIOTI WG03 – loT Standardisation*

3.3.2 Membership Fees

From the discussion on objectives and degrees of participation in the standard setting process in *Section 3.2* we know that organisations may offer different categories of membership and varying fee structures. These can vary across SSOs. We find that membership fee could range from USD 150,000 (for corporate) to USD 110.15 (for individuals). Please refer to *Annexure 4* for a comparison of membership class and fee across some prominent SSOs. A paper by Andrew Undegrove on "the essential guide to standards[94]" categorises the typical range of

[94] Undegrove. A. "Participating in Standard Setting Organizations: Value Propositions, Roles and Strategies", ConsortiumInfo.org. *https://www.consortiuminfo.org/essentialguide/participating1.php*

members into four categories - *strategic members*[95], *technical committee members,* [96]*advisory members*[97] *or informational members*[98]. Leaders of a technology mostly join the strategic or technical committees; followers join the technical or advisory committees and spectators join either as advisory or informational members. However, most SSOs function in a way that meaningful participation may be possible even without joining as the highest category member.

3.3.3 Openness

Openness of SSOs can play a pivotal role in influencing a member's decision to join an organisation. SSOs operate on extremes; on one end membership may be completely reserved, while on the other membership can be completely open to public. In between there are categories that provide safeguards for accreditation and accommodation of multiple stakeholders. *Figure 3.3* categorizes SSOs into four types (i) open to public (ii) open by formal membership (iii) restrictive membership (iv) reserved. Examples of organisations falling within these four categories have also been included in the illustration. In order to encourage participations, most organisations keep their membership open. However, openness to membership might vary by membership categories. An SSO may be open to all participants in a general category but restrict membership for higher categories such as strategic members or technical committee members. Organisations that adopt a restrictive membership model may be guided by interests of collusion or a refusal to deal with competitors. It is however legitimized on grounds of preserving neutrality, reducing concerns of capture, limiting free riding, etc.[99]Recently, the US government added Huawei to its Entity List; companies on this list can only be partnered or engaged with through a special license. This effectively banned all business between US companies with the Chinese company.[100] Following the ban, the company was removed from some elite global SSOs including the SD Association and the Wi-Fi Alliance Group. Huawei itself suspended its participation from the JEDEC group.[101]There is limited precedence that suggests banning of an entity on security grounds. Despite national security concerns, countries including India, Canada, New Zealand, Sweden, U.K haven't banned Huawei yet nor have many other global SSOs. Using geo-political strategies to fragment the standards eco system is not yet commonplace. However, a good governance system should create checks and balances that discourage SSOs from deliberately excluding rivals, including government pressure, to offer its members significant market advantage.

---

95 Benefits: Guaranteed board seat, or reasonable likelihood of eventually gaining one (total board seats for this class: 9); can nominate officers and committee chairs; and all privileges of lower categories of membership (other than the right to vote for additional directors). Appeal to: Companies (usually vendors) that wish to set the strategic objectives of the consortium. Fees: USD 25,000 – USD 50,000, depending on revenues of member

96 Full, voting participation in all technical and marketing processes; as a class, can elect three board representatives (perhaps with the type of member specified, to ensure diversity of representation); may be invited to provide a committee chair; all privileges of lower categories of membership
Appeals to: Companies, universities, colleges, and government agencies wishing to influence the standards that are developed
Cost: $15,000 - $25,000, depending on revenues or type of member

97 Full non-voting participation in all technical and marketing processes; all privileges of lower categories of membership
Appeals to: All types of members that wish to participate in, but do not need to influence, the technical process, and that wish to have the most timely information regarding technical direction and results
Cost: $10,000 (regardless of revenues)

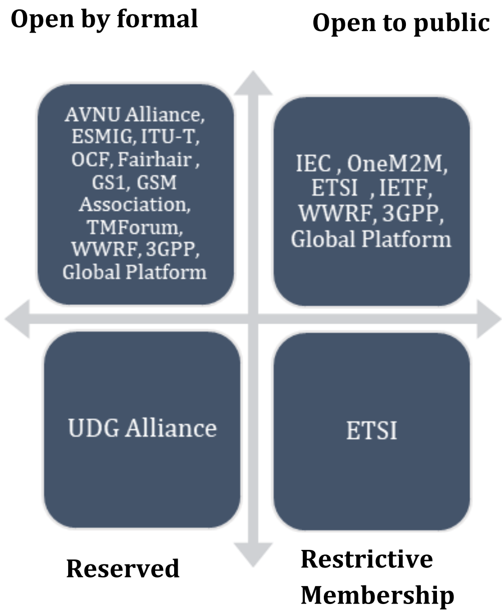
98 Receives periodic information regarding technical and other programs, as well as standards as they are made public
Appeals to: Academics, consultants, analysts, individuals
Cost: $250 (regardless of revenues)

99 Michael Carrier, 2009, "Innovation for the 21st Century: Harnessing the Power of Intellectual Property and Antitrust Law", Oxford University Press

100 http://www.chinadaily.com.cn/a/201905/31/WS5cf06cb5a3104842260bec7c.html

101 https://gadgets.ndtv.com/mobiles/news/uawei-sd-association-wi-fi-alliance-jedec-phones-nexus-6p-removed-from-android-enterprise-device-lis-2042835

Figure 3.3: Openness of SSOs and Alliances



Source: *Compiled by authors from Alliance for Internet of Things Innovation (AIOTI) 2019*

3.3.4 Policies, norms, guidelines and good practices

New standards must be subject to adequate scrutiny to guard against anti-competitive or anti-welfare outcomes. Standards must consider all economic, environmental, health and safety concerns. Accordingly, standard setting organisations follow guidelines for a balanced representation of stakeholders, the mechanism to reach consensus revision of standards, etc. Organisations also adopt formal certification processes or conduct tests to adhere to compliance requirements for standards adoption. For instance, oneM2M hosts events to test interoperability. In the 2018 Interop 6 event, new tests were introduced, including *announcement; time Series, polling Channel*, etc.[102]. For security testing and certifications, standards bodies may collaborate with security evaluation laboratories. One such instance is the collaboration between OneM2M and the Global Platform's Security Certification program[103]. The certification program ensures that the standards components meet the required levels of security defined for a service. The security testing is available at three levels – Basic, Enhanced and High. Similarly, Kyrio is an Authorised Testing Lab (ATL) for the Open Connectivity Foundation (OCF). It provides a certification program that helps ensure security and interoperability for Internet of Things (IoT) devices. Some SSOs including the GSM Association, ITU-T, WWRF etc. don't follow a laid-out certification process. The adoption of compliance and certification activities may also influence the participation and membership in SSOs. Please refer to *Appendix 4*for a summary of testing and certification processes adopted by a select set of SSOs.

3.3.5 Ratification

Standard setting bodies follow due process - *guidelines and ethical constraints placed on their administrative decision making*, for approval and adoption of standards. This trusted process of ratification differs widely across SSOs. IEEE's

---

102 oneM2M expands interoperability testing in response to huge IoT growth, June 7, 2018.http://www.onem2m.org/news-events/newsmenu/news/178-onem2m-expands-interoperability-testing-in-response-to-huge-iot-growth

103 https://globalplatform.org/certifications/security-certification/

process is rooted in consensus[104] with a right to appeal, creating an open and balanced environment. It is a six-stage process[105] that requires at least 75 percent of all ballots from a balloting group to bear a "yes" vote. Similarly, ETSI follows a five-stage process (Inception- Conception- Drafting- Adoption-Promotion) for the Technical Organization's production of standards and deliverables[106]. A standard is adopted if at least 71 % of the weighted member votes are in favor of the draft. The IEC's process for standard development also goes through 7 stages (Preliminary – Proposal – Preparatory – Committee – Enquiry – Approval – Publication). In the Enquiry Stage a Final Draft International Standard (FDIS) is circulated for approval[107]. The ratification process for some SSOs is open for external consultation. Table 3.5 below list out the details of SSOs which permit only participation from members in a closed process or consult external parties as well. The robustness of the ratification process is central to the success of an SSO.

Table 3.5: Ratification process followed across SDOs and Alliances

IoT Alliances/ Consortia / Standard Bodies	Closed process done by members only with no consultation from external parties	Done by members and open for consultation from external parties.	Open process for all parties interested in the ratification.
3GPP (3rd Generation Partnership Project)		√	
AVNU Alliance		√	
The European Smart Energy Solution Provider (ESMIG)			√
ETSI (European Telecommunications Standards Institute)		√	
Fairhair[108]	√		
Global Platform		√	
GS1		√[109]	
GSMA (GSM Association)	√		
IEC (International Electro technical Commission)		√	
IETF WG 6lo (IPv6 over Networks of Resource-constrained Nodes)			√

104 Each Balloter has one vote. A standard will pass if at least 75 percent of all ballots from a balloting group are returned and if 75 percent of these bear a "yes" vote. If ballot returns of 30 percent are abstentions, the ballot fails. Ballots usually last 30 to 60 days. Balloters can approve, disapprove, or abstain. They can also approve or disapprove with comments. Balloting is done through myBallot system — an automated service providing an electronic, web-based standards balloting service.

105 Six stage lifecycle diagrams: 1) Initiating the Project 2). Mobilizing the Working Group 3.) Drafting the Standard 4) Balloting the standards 5) Gaining Final approval 6) Maintaining the

106 A proposal for a work item may come from inside or outside the Technical Body. The Technical Body may approve the work item, if at least four ETSI Members volunteer to support the work. The adoption is formally done by the ETSI Membership (the existence of new work items is made known via the ETSI Web site and Members who disagree with the item may within a 30-day period oppose its adoption into the ETSI Work Programme.

107 The FDIS is circulated to the National Committees for a two-month voting period. Each National Committee's vote must be explicit: positive, negative or abstention. No comments are allowed with a positive vote. An FDIS is approved if: 2/3 majority of P-members voting approve and if, less than 25% of all votes submitted are negative. If the document is approved, it progresses to the final publication stage.

108 By general assembly in accordance to voting rules.

109 Done primarily by members but external parties may submit comments

IETF WG 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e)			√
IETF WG ACE (Authentication and Authorization for Constrained Environments)	√		√
International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T)	√[110]		
(ISO/IEC) JTC1/WG10 Internet of Things	√[111]		
OCF (Open Connectivity Foundation)	√		
OneM2M		√	
TMForum	√[112]		
WWRF (Wireless World Research Forum)	√		
UDG Alliance	√		

Source: Compiled by authors from Alliance for Internet of Things Innovation (AIOTI) 2019

3.3.6 Intellectual Property Rights

Companies are constantly investing in development of new technologies and products to stay ahead of competition. These innovations are protected by intellectual property rights (IPRs) accorded through national and international legislation. License agreements and payment of royalties allow for the authorized use of patented standards. The technical committee of SSOs negotiates licenses with users of the standards on *fair, reasonable and non-discriminatory* (FRAND) or royalty free (RF) terms and conditions. The FRAND commitment[113] is the most popular and widely used licensing commitment among SSOs. ITU's patent policy gives patent holders the choice to select between (i) RF (ii) FRAND or(iii) unwilling to license[114]. IEEE-SA Standards Board Bylaws provides two options for submitting essential patent claims - the submitter can either assure not to enforce the patent or commit to license it under FRAND terms[115] . The ETSI IPR policy also requires licenses for essential IPRs to be licensed under FRAND terms[116].

110 Closed process done by members only with no consultation from external parties. NOTE – In some specific cases, it can be done by members and open for consultation from external parties, previous agreement with the external parties

111 Every formal step in developing of the standard is done by national experts. The documents are casted and formally voted and commented on by national bodies. Comments and votes are being handled according to ISO/IEC Directives by the national body in charge of the secretariat.

112 Closed process done by members only with no consultation from external parties. NOTE – In some specific cases, it can be done by members and open for consultation from external parties, previous agreement with the external parties

113 The FRAND commitment gives right holders more power in terms of exclusivity over their patents. They could negotiate on terms and royalty fees under it, whereas they will lose more exclusivity of their patents under RF (not be able to collect royalty) or NAC (not be able to exclude others from use, thus not be able to collect royalty).

114 Annex 2, ITU, 'Guidelines for Implementation of the Common Patent Policy for ITU-T/ITU-R/ISO/IEC'

115 Article 6, IEEE (n 21).This approach is equivalent to the "Non-Assertion Covenant (NAC)" term in the academic literature; see Rudi Bekkers, Eric Iversen and Knut Blind, 'Emerging Ways to Address the Reemerging Conflict between Patenting and Technological Standardization' (2012) 21 Industrial and Corporate Change 901.

116 Article 6, ETSI, 'ETSI Intellectual Property Rights Policy' (n 43).

SSOs also have different policies on copyright. Copyrights provide many exclusive rights, such as the right to enjoin others from having access to, using, modifying and distributing a copyrighted specification. As a copyright owner, an SSO can charge firms or third parties for their access to and use of technical standards. Based on the IPR policies adopted by SSOs, different business models have emerged. ETSI and ITU have made their specifications available for free, whereas IEEE sells its standards[117]. *Table 3.6* below summarises the IPR policy choices for a select group of SSOs.

Table 3.6: Policies on Intellectual Property Rights across SSOs

IoT Alliances/ Consortia / Standard Bodies	IPR Policy
3GPP (3rd Generation Partnership Project)	Individual Members should declare to their Organizational Partners any IPRs which they believe to be essential, or potentially essential, to any work being conducted within 3GPP. During each 3GPP meeting (TSGs and WGs) a call for IPRs must be made by the Chairman using standard wording.
AVNU Alliance	FRAND (fair, reasonable and non-discriminatory) Policy
The European Smart Energy Solution Provider (ESMIG)	No IPR policy
ETSI (European Telecommunications Standards Institute)	FRAND – ETSI IPR policy
Fairhair	RAND (Reasonable and Non-Discriminatory) RF License.
Global Platform	FRAND or RAND
GS1	Royalty fee or RAND
GSMA (GSM Association)	GSM Association Intellectual Property Rights Regulations Version 4.0
Hypercat	Creative Commons Attribution 4.0 International License
IEC (International Electro technical Commission)	ITU / ISO / IEC code of practice, FRAND
IEEE Standards Association	The IEEE-SA Patent Policy is section 6 of the IEEE-SA Standards Board Bylaws
IETF (Internet Engineering Task Force)	The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)
International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T)	ITU / ISO / IEC code of practice.
(ISO/IEC) JTC1/WG10 Internet of Things	Common Patent Policy for ITU-T/ITU-R/ISO/IEC and the related "Guidelines for Implementation of the Common Patent Policy for ITU-T/ITU-R/ISO/IEC".
OCF (Open Connectivity Foundation)	FRANDz – Free licensing.

[117] http://ejlt.org/article/view/593/848

OneM2M	FRAND
OSGi Alliance	OSGi specifications are royalty free.
TMForum	TM Forum Code of Practice/Policies
WWRF (Wireless World Research Forum)	WWRF IPR Policy. All IPR generated by members remains with members, WWRF does not seek to own IPR other than copyright of publications and registration of trademarks.
UDG Alliance	Specific access rules defined by the Alliance.

Source: Compiled by authors from Alliance for Internet of Things Innovation (AIOTI) 2019

A comparative analysis of SSOs across these parameters reveals that the governance structures and processes (like ratification, openness and membership fees to name a few) may play a vital role in determining which standard makes it to the fore. This is further complicated by IPR regimes (which FRAND offsets to a great extent) which might impede the voices of start-ups and small-scale enterprises in shaping the narrative of lesser known but relevant standards[118]. While pre-screening of SSOs is important for businesses and contributors to the standard development process, governments must ensure that stakeholders collectively gain from the benefits of participating in the process and catalyse technology development at the macro-level. The focus on governance of SSOs is particularly relevant to India as it prepares to transition from a follower to a contributor for emerging technologies such as IoT. Timothy Simcoe found that voluntary SSOs using a consensus process had become increasingly politicized, crippling standards production for the Internet between 1993 and 2003. He illustrates conflicts motivated by commericialisation of the Internet. The 56K modem was also manufactured using two different standards that were not interoperable. Users and ISPs stayed away from the market until the stalemate was broken by ITU in 1997 by introducing the 'v.90' standard which reconciled the two rival technologies.

Given the plethora of SSOs, a national body like the BIS may assume the role of a trend-setter maximizing participation of the developer community that focuses on India's local technological needs but simultaneously checks for delays in standards production.BIS's membership is open to the public, however after review of organisational details. Its IPR policy is a bit unclear. In case of Indian standards which are technically equivalent or same as International Standards, the IP Policy of the concerned International Standards organisation prevails. The standard activities done by members are open for consultation from external parties and are rooted in consensus. On the other hand, TSDSI's membership is open to public with a fee that varies by entity. They follow FRAND principles after adoption of IPRs. Consultations are also open to external parties. TEC's IPR policy is aligned to ITU's, i.e., either RF or on FRAND terms. The standardisation activities also invite comments from external parties.

The next sub-section highlights case studies elaborating upon the adoption of standards across industrial and consumer IoT applications. These cases seek to identify the adoption of IoT solutions or products in India, the standards deployed in preparing the solutions and also identify challenges unique to the IoT standardisation process in the Indian context.

3.4 Industrial IoT, Consumer IoT and Smart Cities in India

In this section we provide case studies of IoT solutions developed and deployed in India with an emphasis on the standards used. Besides illustrating the role of standardisation in commercialization of IoT solutions in India, the case studies also highlight other roll out challenges for both industrial and consumer IoT solutions in India.

[118] Kapoor. V and Nagpal. P, "Intellectual Property Rights and Small Medium Enterprises (SME's)", International Journal of Law and Legal Jurisprudence Studies, ISSN-2348-8212 http://ijlljs.in/intellectual-property-rights-and-small-medium-enterprises-smes/

3.4.1 Industrial IoT

Industrial IoT (IIoT) is a subset of IoT that uses sensors, computers and networks which interact with their environment to generate data for optimization of industrial applications. With a strong focus on machine to machine (M2M) communication, big data and machine learning, IIoT enables faster and better decision making, increasing efficiency and reliability in industry operations. IIoT applications include smart products, design principles and data driven automation that utilises modern sensor technology to enhance different types of equipment with remote monitoring and maintenance capabilities. It is one of the key elements of industry 4.0 or smart factories.

IIoT has become a strategic priority across various industries including manufacturing, retail, utilities, transport, etc. According to the Morgan Stanley-Automation World Industrial Survey (2015) of 200 automations executive, it was found that the use of IIoT creates new business opportunities, reduces downtime and maximizes asset utilization in the industry[119]. For instance, IIoT enabled machines can self-monitor and predict potential problems which increases overall efficiency of the manufacturing process. The real-time data delivers insights like off-hour consumption and rationalize energy use. Another value addition from IIoT is predictive maintenance (PdM)[120]. PdM indicates when machine or equipment failure might occur – and prevents such occurrences by timely maintenance. IIoT solutions also help monitor supply chain and inventory management. Retailers use IIoT for quick and intelligent marketing decisions across their network of stores. Most applications automatically update consumers' preferences making it easy for retailers to offer smart promotion[121].

Connecting vehicles to the internet has given rise to a wealth of new possibilities, making transport safer and more convenient for users. Key applications in the transport industry are fleet management, vehicle to vehicle and vehicle to infrastructure communication, vehicle pooling and hiring services and self-driving vehicles. Utilities are also investing in technologies such as IoT, robotics process automation (RPA), augmented reality (AR) and virtual reality (VR) and AI to automate maintenance of assets and improve responsiveness towards customer.

According to a report by Software.org[122], adding the augmented reality (AR) dimension to IoT expands its potential. IIoT enables the integration of legacy machinery, commonplace within these complex industries, with powerful IIoT platforms democratising lucrative data for different use cases, roles, and applications. AR provides a new lens to view this real-time data in-situ for a variety of use cases, which ultimately improve front-line worker productivity. AR is finding a natural fit in industrial arenas. The 2019 Survey on the State of Industrial Augmented Reality[123] finds 20% AR respondents in industrial products, 9% in automotive, 7% in electronics & high-tech, and 6% in aerospace & defense. Adding AR into these industrial functions' bolsters worker capabilities, improves productivity and becomes complementary to IIoT. For instance, AR adds a new and immersive human-machine interface (HMI) to IIoT data such as real-time asset monitoring bringing telemetry data into the operator's view to maintain uptime. While IIoT in service (remote monitoring) significantly improves technician efficiencies (truck rolls, remote resolutions). For example, Thyssenkrupp's service technicians use Microsoft HoloLens to visualize real-time data about the health of their elevators, which allows them to make better informed decisions on how to best service the units. Microsoft HoloLens[124][125] is a pair of mixed reality smart glasses developed and manufactured by Microsoft.

---

[119] The Internet of Things and the New Industrial Revolution, Morgan Stanley. April 18, 2016. https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics
[120] https://www.fiixsoftware.com/maintenance-strategies/predictive-maintenance/
[121] https://www.hpe.com/in/en/what-is/industrial-iot.html
[122] https://software.org/press-release/connecting-to-new-opportunities-through-connected-devices/
[123] The State of Industrial Augmented Reality 2019.https://www.ptc.com/-/media/Files/PDFs/Augmented-Reality/State-of-AR-Report-2019.pdf
[124] https://www.microsoft.com/en-us/hololens
[125] HoloLens was the first head-mounted display running the Windows Mixed Reality platform under the Windows 10 computer operating system.

There has been a rapid uptake of IIoT globally. Accenture estimated that IIoT could add USD14.2 trillion to the global economy by 2030, with significant gains for mature economies[126]. The estimated gains for US are USD 7.1 trillion, followed by Germany (USD 700 billion) and United Kingdom (USD531 billion). The IIoT adoption in India is much slower than other countries. Some recent developments and use case include the launch of IoT based asset tracking provided by Tata Communications. Tata Power used data from an internal geographical information system (GIS) to create this solution which provides an asset trace log on a periodic basis and geo-fence breach alerts. It also allows information to be converted into actionable insights in real-time which improves operational efficiencies[127].Similarly, Facilio, an IoT startup provides facility management software that helps commercial real estate property owners maintain infrastructure and ensures that facilitates such as air conditioning systems and elevators are functioning properly[128].Several other companies are providing IIoT solutions in India and it is expected that industrial IoT adoption in India will surpass consumer IoT by 2020.

3.4.1.1 IIoT and the Potential for AR, VR and MR

Augmented Reality (AR) and Virtual Reality (VR) are used extensively in manufacturing design. Some very popular designs are the wing design for Boeing[129], ship design in Finland, etc. Founded in 2010, Queppelin develops AR VR applications in India for clients across industries including manufacturing, pharmaceutical, retail, real estate, training, and education. The platforms of Queppelin include VR-based training solutions for the manufacturing industry, AR furniture retail platform, consumer AR solutions for merchants to create AR marketing experiences and Mixed Reality (MR) applications for pharmaceutical companies. The company also deploys AI/ML and IoT in smart farming. It is based on IoT technologies that enable growers and farmers to reduce waste and enhance productivity. This includes i) collecting data with IoT devices such as pH level indicators, intruder alert, pest, water drainage, ii) process in a central hub through a low-frequency antenna to the central gateway or Neural Network, iii) past data analysis juxtaposed with current data to predict the crop health and assessment, better crop management, iv) see real-time data of field through AR/VR, understand the preventions can be taken, and chat with experts with actual footage of field[130].Similarly, Loop Reality's product Perspect AI helps HR professionals and talent acquisition persons hire the right candidates. The startup uses VR to create assessments that recognize the talent and potential of the recruits and whether they will be the best fit for that company[131]. Recently, to fulfill the needs of ventilators (imported from Germany) in Wuhan amidst the COVID breakout, German manufacturer, Huber & Ranner used BlinkIn's AR[132] product Scotty[133] to provide visual guidance[134].With the help of BlinkIn's AR, hospital staff in Wuhan just had to click on a link to get tech support. When they pointed a phone at the ventilator and installation point, AR markers helped indicate what needed to be done as a technician talked them through the process. Scotty uses WebGL, a JavaScript API, to render graphics on a compatible browser. The AR/VR/MR market is likely to see explosive growth with big companies making serious

---

126 Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015. https://www.accenture.com/t00010101t000000z w /it-it/ acnmedia/pdf-5/accenture-industrial-internet-of-things-positioning-paper-report-2015.pdf

127 Media Release on Tata Power capitalizes on synergies within Tata group - launches IoT based asset tracking solution enabled by Tata Communications, March 9, 2018. https://www.tatapower.com/media/PressReleaseDetails/1501/Tata-Power-capitalizes-on-synergies-within-Tata-group-launches-IoT-based-asset-tracking-solution-enabled-by-Tata-Communications

128 https://facilio.com/

129 https://www.boeing.com/features/2018/01/augmented-reality-01-18.page

130 Choudhury. A (2020). How This Gurugram-Based AR/VR Startup Provides Solutions Integrated With IoT and ML. Analytics India, April 20, 2020.https://analyticsindiamag.com/how-this-gurugram-based-ar-vr-startup-provides-solutions-integrated-with-iot-and-ml/

131 https://perspect.ai/

132 The three-year-old bootstrapped startup in Bangalore, which was initially a consultancy called Etrix, found the ecosystem more favourable in Europe for its products

133 https://scotty.expert/en/about-us/

134 Chakraberty. S(2020) How a Bengaluru startup helped contain the Wuhan outbreak, LiveMint. March 30,2020. https://www.livemint.com/companies/start-ups/how-a-bengaluru-startup-helped-contain-the-wuhan-outbreak-11585507715562.html

commitment to the development of the technology. While application toolkits have been made available to developers there are no standards for AR/VR/MR yet.

There are various formal standards bodies such as IEEE, Video Electronics Standards Association (VESA) and consumer technology association (CTA) who has been involved in VR, AR and MR standards. Other standards bodies such as Society of Motion, Picture and Television Engineers (SMPTE), ITU, Info Comm and Information framework (SID) too have made announcements on VR/AR/MR standards. On May 9th 2018[135], the IEEE announced eight standards in a new P2048 standards family dedicated to VR and AR. These are being undertaken by the IEEE VR and AR Working Group (VRAR). Over time 4 more standards became active as provided in Table 3.7 below. These IEEE standards deal primarily with software issues and interaction of the user with the real and/or virtual world. They are not hardware standards. The IEEE P2048.7 is needed to specify a unified map for various AR and MR applications to assign coordinates, orientations, and other arguments in the real world to virtual objects. The map enables shared use of virtual objects among different users or even among different applications. Similarly, IEEE P2048.4 has use cases in distance education, e-commerce, work meetings, or simulation and training where such a standard helps in consolidating a common virtual identity for a person and provide ways to authenticate the same[136]. IEEE P2048.11 — Standard for Virtual Reality and Augmented Reality: standard defines an overarching framework for AR systems that assist drivers and/or passengers in vehicles. In-vehicle augmented reality has become a new way of providing driving assistance and other infotainment services in vehicles, and is regarded as a promising vertical application of augmented reality. It can be implemented on various devices: Head Up Displays, Smart Glasses, etc. The common point is to make the user interface more friendly while avoiding or minimizing the risk of distracted driving[137].

Table 3.7: Standards Under Considerations for AR and VR

SDOs	Standards on AR and VR
IEEE	• IEEE P2048.1—Device Taxonomy and Definitions • IEEE P2048.2—Immersive Video Taxonomy and Quality Metrics • IEEE P2048.3—Immersive Video File and Stream Formats • IEEE P2048.4—Person Identity • IEEE P2048.5—Environment Safety • IEEE P2048.6—Immersive User Interface • IEEE P2048.7—Map for Virtual Objects in the Real World • IEEE P2048.8—Interoperability Between Virtual Objects and the Real World • IEEE P2048.9 - Standard for Virtual Reality and Augmented Reality: Immersive Audio Taxonomy and Quality Metrics • IEEE P2048.10 - Standard for Virtual Reality and Augmented Reality: Immersive Audio File and Stream Formats • IEEE P2048.11 - Standard for Virtual Reality and Augmented Reality: In-Vehicle Augmented Reality • IEEE P2048.12 - Standard for Virtual Reality and Augmented Reality: Content Ratings and Descriptors • IEEE P3141 - Standard for 3D Body Processing

135 https://www.businesswire.com/news/home/20170509005250/en
136 Yuan. Yu(2017). IEEE P2408 standards paving the road for virtual reality and augmented reality
137 Trivedi. Y (2017).Standards for the Virtual World.https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7992921

CTA	• ANSI/CTA-2087: This document explores XR hardware accessories and their connections. The goal is to agree on common terminology and definitions for XR hardware accessories on a common connectivity standard, including device compatibility. • ANSI/CTA-2085: This document defines the definitions and characteristics for VR Video, and VR Images, which are still or moving imagery captured and formatted explicitly as separate left and right eye images; usually intended for display in a VR headset. • CTA-2069 : Definitions and Characteristics of Augmented and Virtual Reality Technologies
ITU	• ITU-T J.301 specifies requirements that should be considered for augmented reality (AR) smart television system (AR-STV).
3GPP	• 3GPP's subgroup SA4 conducted a feasibility study on virtual reality media services over 3GPP. The technical report can be accessed online[138]. Further, the subgroup SA1 specifies service requirements for the 5G system which includes aspects related to support various VR and AR use cases.

Source: Compiled by authors

The Video Electronics Standards Association (VESA) has formed a special interest group (SIG) to address standardization for the fast-growing AR and VR markets[139]. The Khronos Group has announced the ratification and public release of the Open XR 0.90[140] and provisional specification for royalty-free standards related to augmented reality (AR) and virtual reality VR devices, collectively known as XR. The Open XR 0.90 provisional release specifies a cross-platform application programming interface (API) enabling XR hardware platform vendors to expose the functionality of their runtime systems. By accessing a common set of objects and functions corresponding to application lifecycle, software developers can run their applications across multiple XR systems with minimal porting effort — significantly reducing industry fragmentation.

However, these standards are still to see widespread adoption. There are only handfuls of companies such as Microsoft that are involved in providing solutions, which are mostly proprietary. Given a lack of expertise, there aren't enough developers who can deliver an accessible and useful experience. Privacy and security also pose significant challenges as a result of inconsistencies in augmented reality programming, oversight, and negligence. Another big problem with implementing AR solutions is the technological gap between AR devices. This has limited the use of standards adoption.

3.4.1.2 IIoT Standards

Several national committees and standards organisations involved in developing, prototyping and promoting standards that are needed for development of IIoT solutions/ smart manufacturing. These organizations facilitate consensus building and ensure that standards are openly available to companies that wish to use them. International standards bodies such as International Organization for Standardisation(ISO)[141], International

[138] 3GPP SA4. (2018, January) Virtual Reality (VR) media services over 3GPP. [Online]. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=30 53.

[139] https://www.displaydaily.com/article/display-daily/vr-ar-standards-are-we-confused-yet

[140] https://www.khronos.org/news/press/khronos-releases-openxr-1.0-specification-establishing-a-foundation-for-the-ar-and-vr-ecosystem#:~:text=OpenXR%20is%20a%20unifying%2C%20royalty,as%20XR%E2%80%94platforms%20and%20devices.&text=Now%20is%20the%20time%20for,start%20putting%20OpenXR%20to%20work.%E2%80%9D

[141] An independent, non-governmental standards organisation founded in 1946. ISO 15926, on the topic of "Industrial Automation Systems and Integration," is a key standard that applies to the area of smart manufacturing. Within ISO, the technical committee on automation systems and integration (TC184) has two subcommittees (SC) that are of particular interest in our landscape: SC4 and SC5. SC4 focuses on industrial data standards – primarily those related to product data including ISO 10303. SC5 focuses on interoperability, integration, and architectures for automation applications. Both subcommittees have new standards for smart manufacturing in development.

Electro technical Commission(IEC)[142]and national bodies including professional organizations such as American National Standard Institute (ANSI)[143]in the US , provide some of the leading standards for IIoT. Standards and best practices developed by consortia including Open Applications Group (OAGi)[144], OPC Foundation (OPC)[145], International Society of Automation (ISA)[146]and Manufacturing Enterprise Solutions Association (MESA)[147]are sometimes referred to ISO and IEC for broader dissemination and adoption.

Government sponsored initiatives are also working on developing the smart manufacturing ecosystem in their respective countries. The Smart Manufacturing Leadership Coalition in the US, Industrie 4.0 in Germany and Manufacturing Innovation 3.0 in Korea are some examples. These initiatives are providing the best use of existing standards and identifying and addressing gaps by working with standards development organisations. Complex processes of SSOs and the time-consuming consensus building process has also resulted in the rise of open source standards, often developed within a consortium, maintained collaboratively, but available to the public at large. In India, the drive towards IIoT is primarily driven by Samarth Udyog Bharat 4.0 which aims to spread awareness of Industry 4.0 amongst various Indian manufacturing industries. Five centres tasked with this responsibility are: a) Center for Industry 4.0 (C4i4) Lab Pune; b) IITD-AIA Foundation for Smart Manufacturing; c) I4.0 India at IISc Factory R & D Platform; d) Smart Manufacturing Demo & Development Cell at CMTI; & e) Industry 4.0 projects at DHI CoE in Advanced Manufacturing Technology, IIT Kharagpur[148].

Our interaction with IIoT companies establishes the growing recognition amongst solution providers on the use of standards to establish interoperability and data security across their services in India. For instance, Ascent Intellimation Pvt. Ltd. (AIPL),[149] a Pune based IoT solution provider, provides digital transformation and Industry 4.0 solutions to manufacturing enterprises on an IIoT platform Plant Connect®. Their solution portfolio currently includes:

- Plant Connect SFactory –Smart factory (Industry 4.0) is a solution for manufacturing companies. It provides real time data and analytics for production and maintenance of manufacturing plants and helps improve operations.
- Plant Connect RAMS – Remote Asset Monitoring is a solution for maintenance agencies, equipment rental and utility companies. This solution offers tremendous improvements to after sales service.
- Plant Connect Insights – This solution offers real time data management, web-based MIS reporting, etc. Buyers of this solution include companies from the dairy, food & beverage sector, chemicals, etc.

---

142 The leading international standards organisation focused on electrical, electronic and related technologies; which cooperates with ISO as needed. IEC plays a key role in developing standards for the networking/infrastructure side of the internet of things (IoT). For example, IEC TC 65 focuses on standards for industrial process control and automation and is active in addressing integration between product data and production processes. ISO/IEC Joint Technical Committee (JTC) 1 on information technology deals with a large number of standardization topics in IT for manufacturing systems including sensor and device networks and user interfaces. Consequently, these types of standards are also included in our landscape

143 The American National Standards Institute is a private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States

144 Founded in 1994, it is a not-for-profit open standard development organisation focused on standards for business process interoperability, both inside and between production companies.

145 A foundation made up of the developers of both the OPC, and, more recently, OPC-UA families of standards for the secure, reliable exchange of information in the industrial automation space

146 A nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety and cyber security of modern automation and control systems used across industry and critical infrastructure

147 An associated which play several roles in the development and application of industry standards, and provides guidance in the form of education, whitepapers etc. on the role and application of industry standards for manufacturing systems and related interoperability/integration topics.

148 https://www.samarthudyog-i40.in

149 https://aiplindia.com/

- Enviro Connect – This is an environment data monitoring system for measuring emissions, ambient air quality, water quality and effluent treatment.

These solutions are successfully deployed in over 1000 installations across India and the Middle East. Similarly, B&R Industrial Automation[150], a member of the ABB group is an innovative automation company with headquarters in Austria and offices all around the world. The India office is located in Mumbai. As a global leader in industrial automation, B&R's Industrial IoT solutions offer advantages for both new machinery and equipment (green fields) as well as existing legacy systems (brown field) in three main areas: optimize asset utilistion, add sales potential and optimize services. Some of the solutions offered by B&R includes: *ARPOL PDA, Orange Box, digital remote access, edge architecture/cloud connectivity, asset performance monitor, APROL CONMON, predictive maintenance, digital twin, APROL ENMON, Open Communication, adaptive manufacturing and map technology.* The details are provided in *Appendix 6*.

Smart control [151]is another industrial automation company founded in 1995 that delivers turnkey solutions for process automation, SCADA[152] and IT Integration across several industry verticals including rubber and tyre, automobile, textile, power, metals, food, airport baggage handling etc. Real time data collected using smart sensors and devices help gain real-time visibility into the operational status and performance of the company's assets. The standards used for communication across machine software, hardware, data transmission, data security across all three companies are summarised in Table 3.7 below.

Table 3.7: Standards used by IIoT Companies

Company	Standard Used
B&R Industrial Automation	Open Edge Connectivity: OPC, Modbus, messaging query telemetry transport (MQTT) Connecting computer and its peripheral devices: Ethernet, RS485 (communication interface in data acquisition and control application) and RS232 (a standard protocol used for serial communication) Security Standards : HTTP (Hypertext Transfer Protocol) and Hypertext Transfer Protocol Secure (HTTPS), secure socket layers (SSL) and transport layer security (TLS)
Smart Control	All the internet standards and ISA-95 (security standards)

OPC Unified Architecture (OPC UA) is a vendor-independent communication protocol for industrial automation applications. Since OPC UA is flexible and completely independent, it is regarded as the ideal communication protocol for the implementation of Industry 4.0. Power link is a standard for data transfer, first developed by B&R, and specified as a standard by the open user group Ethernet Power link Standardisation Group (EPSG)[153].Power link has been adopted by the IEEE under IEEE 61158. It is the only Industrial Ethernet protocol to achieve this status. The IEEE views its standards for Time Sensitive Networking (TSN) and Power link as core components for real-time industrial communication. For safety-critical data, the Ethernet Power link can be expanded with the open SAFETY protocol. It is an independent protocol that can be used with all field

150 https://www.br-automation.com/en-in/
151 http://www.smartcontrols.in/download.html
152 A SCADA system is a common industrial process automation system which is used to collect data from instruments and sensors located at remote sites and to transmit data at a central site for either monitoring or controlling purpose
153 https://www.kunbus.com/ethernet-basics.html

buses, Industrial Ethernet solutions or other industry-specific communication solutions for secure transfer of data across industrial environments[154].

The case study interactions not only identified common standards used for IIoT in India, it brought to fore the use of OPC-UA as a new standard being rapidly adopted for Industry 4.0.[155]The standard is open source and available free of cost. With OPC-UA, Ethernet time sensitive networking (TSN), real time data for automation and robotics application would be possible. This will provide vendor independent end-to-end interoperability into field level devices for all relevant industry automation use-cases. The main feature of TSN is the possibility of coexistence of different traffic types, while maintaining the timing properties of real-time traffic. Some existing real-time technologies (EtherNet/IP, Profinet) use traffic planning and quality of service to ensure real-time behavior under the condition of well-behaving devices. With TSN as data link layer, those technologies can leverage better bandwidth efficiency, since TSN protects the high priority traffic unconditionally[156].

The use of OPC-UA has also been promoted by the Bureau of Indian standards (BIS)[157]. Currently, the adoption of OPC-UA solutions is limited only to large scale companies in India. The small and medium enterprises lack awareness on availability of such standards. Beside most companies using IoT solutions are still working with previous generation machines that are not compatible with new standards. However, companies like B& R also offer solutions such as “orange box” that brings smart-factory intelligence to brown field installations. This makes it possible to read and analyze data from previously unconnected machinery and equipment. Standardisation will help scale the availability of such technologies and make it affordable for more Indian companies to upgrade their machines and reap benefits of Industry 4.0.

Some other standards that belonged to the IIoT space and are being used by Indian companies are listed in Table 3.8.

Table 3.8: Standards used on IIoT

Standard	Organisation	Description
Industrial Internet Reference Architecture V 1.9	Industrial Internet Consortium (IIC)	This architectural standard provides a common framework and concepts for IIoT architects to develop interoperable IIoT systems across different Industry verticals
ISA95 Enterprise-Control System Integration	International Society for Automation (ISA)	This refers to a series of standards developed for global manufacturers to develop an automated interface between an enterprise and its control systems. All the pertinent standards have been distributed across different processes and are available on the ISA website

154 https://www.ethernet-powerlink.org/fileadmin/user_upload/Dokumente/Downloads/POWERLINK_FACTS/POWERLINKFacts_01_10_Englisch_Edition__1_.pdf

155 Hoppe. S (2017). There Is No Industry 4.0 without OPC UA, Automation.com https://www.automation.com/automation-news/article/there-is-no-industry-40-without-opc-ua

156 OPC UA TSN A New Solution for Industrial Communication. https://www.automationworld.com/home/whitepaper/13318642/opc-ua-tsn-a-new-solution-for-industrial-communication

157 Pre-Standardization Study Report on Smart Manufacturing

ISA88 Batch Control	International Society of Automation (ISA)	This refers to a series of standards that defines all the models and terminology of batch process control during batch production.
ISA/IEC 62443 Cybersecurity Certificate Programs	International Society of Automation (ISA)	Refers to a series of four certificate programs for those involved in IIoT. The Certification program is designed to increase the market's recognition towards adopting security fundamentals embedded in the ANSI/ISA99 Industrial Automation and Control Systems Security standard.

Compiled from the websites of ISA, IIC, &PLC Academy

Besides these prominent standards, IEEE standards are also used for IIoT applications. These include (i) IEEE 2413: IEEE Standard for an Architectural Framework for the Internet of Things (IoT), (ii) IEEE P1451-99: Standard for Harmonization of Internet of Things (IoT) Devices and Systems, (iii) IEEE P2755.1 - Taxonomy and Classification for Software Based Intelligent Process Automation (SBIPA) Technology, (iv) IEEE P2755.1 - Taxonomy and Classification for Software Based Intelligent Process Automation (SBIPA) Technology, (v) IEEE P2672: Guide for General Requirements of Mass Customization, (vi) IEEE P2755.1 - Taxonomy and Classification for Software Based Intelligent Process Automation (SBIPA) Technology, (vii) IEEE 2301 Guide for Cloud Portability and Interoperability Profiles (CPIP), (viii) IEEE 1934 - IEEE Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing, (ix) IEEE 802.1 - Time Sensitive Networking Group, (x) IEEE P1931.1: Standard for an Architectural Framework for Real-time Onsite Operations Facilitation (ROOF) for the Internet of Things and (xi) IEEE P2671: Standard for General Requirements of Online Detection Based on Machine Vision in Intelligent Manufacturing.

3.4.2 Consumer IoT

With rapid innovations in the IoT space, the impact of IoT on consumer products has moved from hype to reality. IoT devices are no longer luxury, a variety of IoT systems and devices such as Google Nest, Fitbit bands, home appliances, public transit systems, energy meters etc. have become a part of daily life, at least for urban dwellers. Technological advancements such as 5G will pave the way for continued innovation in this market. As per GSMA's Intelligence Report, almost11.4 billion consumer IoT devices would be available by 2025. The consumer survey on IoT trends in 2018 revealed that the number of personal IoT devices in 2017 was around 5.2 billion, with digital assistants, smart glasses and augmented body, experiencing the highest growth rates since 2016[158]. The smart home products and services are also on the rise and it is expected that the smart home market will grow from USD 35.7 billion in 2017 to USD 150.6 billion by 2023, with global market for smart home security growing at 27 per cent annually. Google, Apple, Amazon, Roku TV and iRobot are some of the biggest players in the smart home segment[159].

[158] IoT Trend Research: The Evolution of Consumer IoT. Reply. https://www.reply.com/Documents/SONAR_research/IoT_trends2018_the_survey_on_consumer_EN_IoT_Reply.pdf

[159] *Ibid*

India, though still nascent, has also observed some growth in consumer IoT. At least 9.5 percent of Indian homes are expected to be outfitted with smart devices by the end of 2023[160]. According to International Data Corporation (IDC)'s India Monthly Smart Speaker Device Tracker, a total of 7.53 lakhs units of smart speakers were shipped in 2018 in India[161].Though the smart speaker is a relatively young product in India, the integration of voice assistants such as Alexa and Google Assistant in smart devices is gaining immense popularity in the country. Further the smart meter national program aims to retrofit 25 crore conventional meters with smart variants over three years which is expected to bring 80-100 per cent improvement in billing efficiency in Indian homes[162]. The connected car market in India is currently sized at USD 1048 million and is projected to reach USD 32.5 billion by 2025.[163,164]High cost and data privacy are the primary concerns limiting the uptake of consumer IoT in India. Instances of system hacking and data leaks have raised serious concerns regarding IoT security.[165] Consequently much of the recent standardisation efforts are focusing on the security of IoT devices. Adding AR and VR dimensions to Consumer IoT, expands its potential, especially in gaming and entertainment applications. India has been slow to wake up to its potential, with most Indian startups in the field, still focused on making a mark in the VR segment of the market. In the last few years, only about 170 startups have emerged in this space. However, in the next five years, this industry is likely to see a compounded annual growth rate of 76%. FlippAR a startup, for instance, uses the phone GPS and camera to display additional information, such as reviews and promotions about a restaurant that the user is near. It can also help users by supplementing them with information about known landmarks by scanning using the mobile phone camera.

The present IoT solutions and products lack standards for handling unstructured data and ensuring its security. For instance, outdated protocols and the lack of data security systems in smart utility solutions can lead to frauds such as overbilling, explosions and house fires. Despite significant effort in this area, there continue to remain gaps in communication standards. Current communication and interconnection standards and regulations are inadequate to address data interfacing requirements. Smart devices manufactured by different companies often lack standards for integration and interoperability. In the Connected Home and Building Technology Trends survey by Jabil[166](2018), 43 percent participants stated the lack of data communication and application standards as one of the biggest challenges. There are well established wireless networking specifications such as Wi-Fi, Bluetooth, Zig Bee and Z-wave as well as new protocols including X10, Insteon, Thread, and Universal Power Line Bus (UPB) in the home segment. However, the absence of an overarching or leading standard is a reported challenge that the sector is facing.

Open Connectivity Foundation will provide the first international smart home standard to ensure robust and secure connectivity by completion of OCF 2.1 certification[167] in 2020.This will enable the development of vertical IoT devices for both smart homes and smart commercial devices while maintaining fundamental interoperability between device architectures. OCF was established in February 2016 by Samsung Electronics, Intel, Microsoft, Qualcomm and Electrolux to develop a framework which enabled interoperability of IoT devices through a

---

160 Chowdhary. S (2019). "Home automations: Making our homes smart and connected", Financial Express, June 6, 2019. https://www.financialexpress.com/industry/technology/home-automations-making-our-homes-smart-and-connected/1599137/

161 India Smart Speakers market touches a new high in 2018, IDC India Reports, March 28, 2019. https://www.idc.com/getdoc.jsp?containerId=prAP44965119

162 Smart Meter National Program.http://vikaspedia.in/energy/policy-support/energy-efficiency/smart-meter-national-programme

163 PRNewswire (2019). "India Connected Car Markets, 2019-2025 - Emerging Profit Pool for Automotive Industry", Research and Markets.com's. September 2, 2019 https://www.prnewswire.com/news-releases/india-connected-car-markets-2019-2025---emerging-profit-pool-for-automotive-industry-300910154.html

164 Statista

165 The state of IoT Security. https://www2.gemalto.com/iot/iot-consumer-insights.html

166 https://www.jabil.com/forms/connected-home-building-tech-trends.html

167 The OCF Universal Cloud Interface (UCI) is a programming interface that can be used to standardise connectivity between different manufacturers' cloud servers. It is based on the OCF's proximity framework that supports communication between IoT devices and applications over a local network. It uses the same data models and core technology.

standard specification, reference open source implementation and a certification program. It is also designed to act as a common translation layer between non-OCF devices and protocols. Prior to OCF, companies were operating in silos either as a part of OIC or the AllSeen Alliance. Under the OCF, these groups are working towards a single standard which not only supports new devices but is also working towards backward compatibility with older devices. The members of the OCF and their affiliates can license their specifications on royalty-free or nondiscriminatory terms. One M2M and OCF have also developed harmonized standards to permit seamless interworking between oneM2M and OCF environments. This provides a standardized way to create interoperable IoT systems that can address both local and wide-area network scenarios.

The OCF India chapter was launched on May 10th, 2019. Samsung Research and Development Institute in partnership with Nasscom, Intel and L&T announced the formation of the OCF India Ecosystem Task Force to increase awareness about global Internet of Things (IoT) standards and its benefits for the Indian IoT Industry[168]. Samsung being one of the founding members of the OCF, since 2014, has been contributing to OCF standards development and also adopting OCF specifications in its IoT device ecosystem. With Bixby[169], the virtual assistant developed by Samsung Electronics, the company is planning to infuse AI for a harmonized IoT experience at home. Some of the Bixby-enabled devices that Samsung plans to bring in India are the Smart 4K QLED[170] Televisions and Refrigerators called the "Family Hub[171]" that could operate on a single connected cloud platform called the "Smart Thing Cloud" which will control and monitor connected devices.

Since India is vulnerable to IoT attacks, product development must prioritise security of devices. Security is one of the primary reasons for the slow adoption of consumer IoT in India.[172] IoT vendors must necessarily layer their networks with security to earn consumers trust. This will go a long way in paving the way for large scale adoption of consumer IoT in India.

3.4.3 Smart City

ITU defines sustainable smart cities as innovative cities that use information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects[173].The scale of smart city deployments demands integration and interoperability across various systems of city governance. Standards enable seamless interaction between technologies and suppliers of components for data and communication management in a smart city project.

The Smart Cities Mission in India aims to promote sustainable and inclusive development of cities. The area-based development aims to transform and redevelop existing cities into better planned ones through the application of smart solutions. The strategic components include city improvement (retrofitting), city renewal (redevelopment) and city extension (green field development). The core infrastructure components of a smart city

168 Balaji. S (2019). "OCF India Chapter: India's IoT market is ready for standardization norms", Nasscom Community, May 21, 2019. https://community.nasscom.in/communities/iot-ai/ocf-india-chapter-indias-iot-market-is-ready-for-standardization-norms.html

169 A huge part of the Bixby development was done at SRI-Bangalore -- the company's largest Research and Development facility outside South Korea. The company has two more R&D centers in Noida. "Bixby-enabled smartphones are here and the technology will naturally metamorphose into other home devices. Bix

170 Voice commands to 'Bixby' can help find favourite movies or songs -- along with controlling compatible IoT home devices like a robotic vacuum cleaner or cameras inside home

171 Bixby-enabled "Family Hub" refrigerators offer a wide range of smart features like syncing food storage with meal preparation, and keeping family members better connected and organised. The refrigerators are able to recognise individual voices of family members and give personalised information such as news, weather and calendar updates.

172 IoT Landscape and Nasscom Initiatives, May 2017. https://www.wfeo.org/wp-content/uploads/stc-information/L3-IoT_Landscape-by-S_Malhotra.pdf

173 ISO-IEC JCT 1 Information Technology: Smart Cities, Preliminary Report 2014.

include *adequate water supply, assured electricity supply, sanitation, including solid waste management, efficient urban mobility and public transport, affordable housing, especially for the poor, robust IT connectivity and digitalization, good governance, especially e-Governance and citizen participation, sustainable environment, safety and security of citizens, particularly women, children and the elderly, and health and education.* Each of these involves the use of technology, information and data to improve the quality of services. For instance, the smart public transport system provides daily commuters information on seating availability, current location of the bus, time to destination, next bus-stop, passenger density, etc.

India has identified 100 smart cities under the Smart Cities Mission at a total project cost of INR 2,05,018 crore[174]. Of the total cost, 80.8 percent is for pan city development and 19.2% is accounted for area-based development[175]. The pan city solutions identified by 20 smart cities are provided in *Appendix 7 and Appendix 8.* At present vertical solutions such as transportation, water, power and waste management are managed by single vendors. For affordable and sustainable solutions an interconnected solution must be developed, that uses open, common and shareable platforms. Standards become non-negotiable components of an integrated city system that uses common infrastructure. Some of the global standards might need local contextualizing before being adopted in India. The sub-section below provides an overview on the key smart cities standards developed by leading organisations and the national standardisation bodies of several countries that could be adopted or developed by national standards bodies in India.

3.4.3.1 Key Smart Cities Standards

At present ISO, IEC and ITU are the three main international bodies that qualify as standards bodies for smart cities. At ISO, Technical Committee 268, constituted in March 2012, under the field of Sustainable Development in Communities, undertakes all smart city related standardisation work.[176]It encourages the development and implementation of holistic, cross-sector and area-based approaches to sustainable development. The standards developed by the committee are summarised in *Appendix 9.1*. IEC's standardisation management board (SMB) formed a system evaluation group in June 2013 that is currently preparing a reference architecture and standardisation roadmap in cooperation with different organisations, fora and consortia. Many IEC technical committees also enable the development of smart cities that is summarised in *Appendix 9.2*. At ITU, ITU-T Study Group 5 (SG5) established a focus group on Sustainable Smart Cities (FG-SSC) in February 2013. A report published by this group in 2014, 'Smart Sustainable Cities: An Analysis of Definitions[177]', introduced ICT as a solution to economic and environmental problems in urban areas. FG-SSC has four main Working Groups (WGs) (i) WG1 – ICT and roadmap for smart sustainable cities (ii) WG2 – ICT infrastructure (iii) WG3 – Standardisation gaps, KPIs and metrics (iv) WG4 – Policy and positioning. However, these international standards by ISO, IEC and ITU broadly cover indicators on smart urban infrastructure and do not address other relevant standards which relate to city services. This reflects a lack of global integration for smart cities standards.

Besides the three international steering bodies, standards for smart cities, including for smart grids, smart metering, 3D video standards, smart vehicles, etc. are also being developed by IEEE, to enable consumer connectivity[178]. IEEE P2413 is a critical standard providing an architectural framework for various IoT verticals. Various other IEEE standards included IEEE P1930.1 - recommended practice for software defined networking (SDN)

---

174 The total cost of projects proposed under the various smart city plans of the 90 winner cities is Rs 1.9 lakh crore. About 42% of this amount is funded from central and state, 23% through private investments and PPPs, and 19% through convergence with other schemes (such as HRIDAY, AMRUT, Swachh Bharat-Urban). The remaining will be generated by the cities through the levy of local taxes, and user fees.

175 *Ibid*

176 ISO/TC 268 Sustainable development in communities, http://www.iso.org/iso/iso_technical_committee?commid=656906

177 Source: http://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/Approved_Deliverables/TR-Definitions.docx

178 S mart Cities – Standardization. http://archive.energy.gov.il/Subjects/EnergyConservation/Documents/SmartCity/MichalPhilosoph.pdf

based middleware for control and management of wireless networks, IEEE P2784 - guide for the technology and process framework for planning a smart city, IEEE P1950.1 - standard for communications architectural functional framework for smart cities, IEEE P1951.1 - Standard For Smart City Component Systems Discovery And Semantic Exchange Of Objectives, IEEE P2872 - standard for interoperable and secure wireless local area network (WLAN) infrastructure and architecture. Based on the stakeholder consultation we found that India through its experts are also leading some of the efforts in Smart Cities (IEEE P1951.1) on Smart Infrastructure and also through many pre-standardisation efforts within Industrial AI, Intelligent Transport Systems testbeds, etc.

Apart from the international standard setting bodies, many countries are developing standards to address the growth of smart cities across the globe. For instance, the British Standards Institution (BSI) in UK is working on a Smart Cities Standards Strategy to identify vectors of smart city development where standards are needed. Several standards including PAS 180 for smart city terminology[179], PAS 181[180] for smart city framework, guidance for decision makers in smart cities and communities, PAS 182for a data concept model for smart cities etc. have already been published. Similarly, AENOR[181] in Spain has issued two new standards on smart cities - the UNE 178303 and UNE-ISO 37120. These standards joined the already published UNE 178301. Several national standardisation committees and consortia have started standardisation work for smart cities. In 2012, the European standardisation organizations CEN and CENELEC founded the Smart and Sustainable Cities and Communities Coordination Group (SSCC-CG) to coordinate standardisation activities and foster collaboration.[182] While the SSCC-CG does not itself develop standards, the joint working group on standards for Smart Grids has provided strategic reports that outline the standardisation requirements for implementing the European vison for smart grids[183]. The details of the country led initiatives are provided in *Appendix 9.3*.

In India, the Bureau of India Standards (BIS) and the Telecommunications Standards Development Society India (TSDSI)[184] have formed dedicated working groups for standards on M2M, IoT and Smart Infrastructure. In 2015, the Civil Engineering Department of BIS set up a technical committee under the chairmanship of Mr. Sudhir Krishna to take up standardisation for smart cities in 2015. In 2016, BIS provided a draft list of smart city indicators across 17 sectors with 46 core indicators and 47 supporting indicators[185]. The guidelines are based on ISO 37120:2014. A pre standardisation study titled "Technical Requirement Analysis of Unified, Secured and Resilient ICT Framework for Smart Infrastructure" was released in November 2017. These efforts are yet to see

---

179 PAS 180 Smart city Vocabulary https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-180-smart-cities-terminology/

180 PAS 181 Smart City Framework https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/

181 https://www.aenor.com/

182 Orchestrating infrastructure for sustainable Smart Cities, http://www.iec.ch/whitepaper/pdf/iecWP-smartcities-LR-en.pdf

183 Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids, https://www.etsi.org/WebSite/document/Report_CENCLCETSI_Standards_Smart%20Grids.pdf

184 TSDSI is an Organizational Partner (OP) of 3GPP and Partner Type1 of oneM2M, and provides all its members with access to these two bodies. BIS is a founder member of International Organization for Standardization (ISO) and member of International Electro technical Commission (IEC) since 1949

185 https://factly.in/bis-releases-draft-smart-city-indicators/

Box 1: LMLC Use Case and RIT for IMT 2020: A Case Study

While India might not be deemed as a major contributor to the overall IoT Standardisation landscape, it is at the vanguard of leading standardisation efforts in the telecommunications sector. Telecommunications, especially 5G, is a critical technology that is essential for developing a robust and resilient IoT infrastructure.

TSDSI was established in 2014 to fill the gap of an apex SDO (highlighted in the National Telecom Policy 2012) which would contribute to the development of next generation telecom standards and drive the ecosystem of IP creation in India[1]. Shortly in 2017, it did manage to achieve these objectives when the International Telecommunications Union (ITU) listed LMLC (Low Mobility Large Cell) use case as a mandatory requirement for IMT 2020 (colloquially known as 5G). Furthermore, TSDSI also introduced its 5G candidate standard called TSDSI RIT (Radio Interface Technology) as a proposal for IMT 2020 which would enable longer coverage for meeting the newly set LMLC requirements[1]. To contextualise these achievements, one must understand the changes that these standards bought about to the existing technological landscape in India.

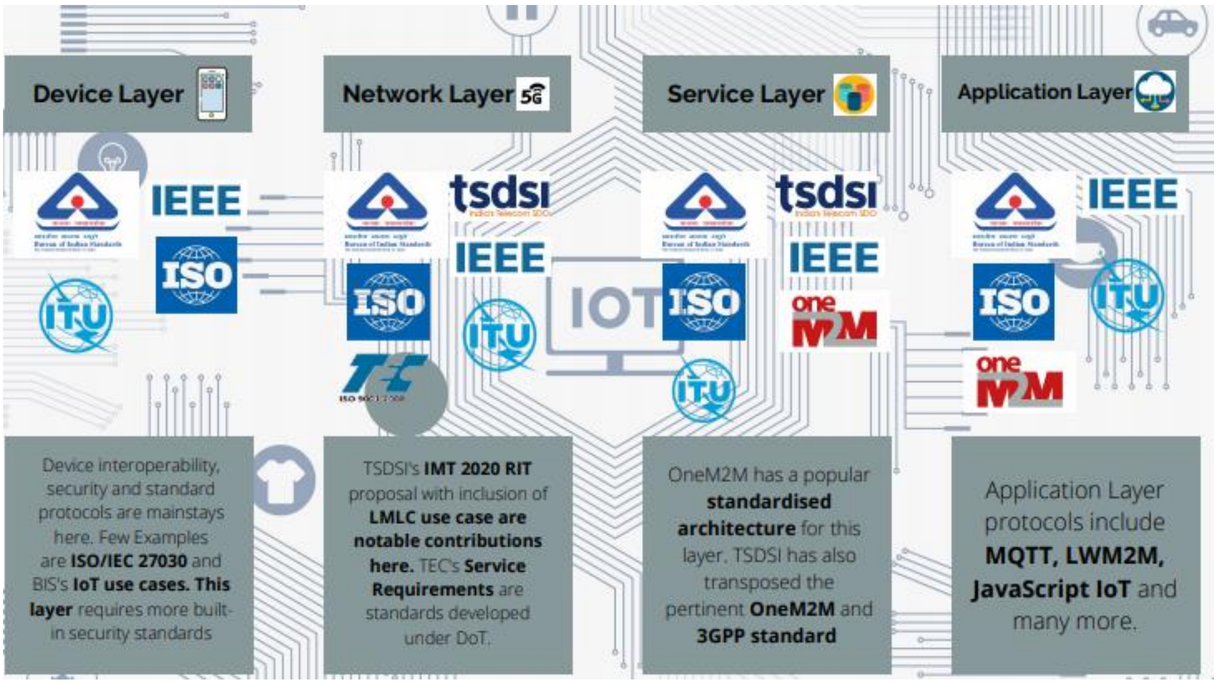
According to the Telecom Statistics of India 2019[1], India had 1183.41 million telecom subscribers as of March 2019, out of which 514.27 million were subscribers who hailed from rural areas. This indicates that there is a strong rural user base in India for the telecom industry. However, significant differences are observed in telecommunications infrastructure [measured by Base stations or BS in technical parlance] between urban areas and rural areas. In a telecommunication network, the network is distributed over land areas called 'cells'[1] which is usually supported by one BS. To increase data transmission rates, small cells supported by multiple BS are used which is conducive for most developed countries and Indian urban areas as the potential revenue for telecom providers is high in such regions. However, in rural areas where there are different climatic conditions and potentially low revenues, setting up numerous base stations in rural areas is seen as financially exhaustive by most industry players[1].To solve for this problem, the Indian government via its Bharath Net Initiative, provided optical fiber connectivity to 250,000gram panchayat villages (out of a total of 650,000 Indian Villages) and installed cell towers to enable wireless connectivity to the neighboring villages left out of the scheme[1]. This implies the presence of large cells with few BS for the rural telecom sector.

Now, if one looks at the standardisation work around LTE before 2017, it is observed that most of the standardisation work was geared towards smaller cells and the definition of rural use cases was tailor-made to the conditions of rural areas of the developed world. This is evident in ITU's original rural test bed requirement which focused exclusively on high speed mobility (120 km) in rural areas and was not reflective of telecom requirements of rural areas in developing countries like India[1]. This would imply that as standardisation work on wireless technologies like 5G would progress, it would inadvertently ostracize most rural areas of developing countries from deriving utility gains from such technological advances. TSDSI's introduction of LMLC as a use case precluded exactly that. The LMLC configuration focuses on low mobility users (a mix of pedestrian with speeds less than 3 kmph and vehicles at 30 kmph) and an inter-base station distance upward of 6 km[1]. This is more indicative of the Indian rural telecom landscape which is characterised by low mobility and high indoor usage. This configuration's inclusion has multiple benefits: a) It updates the rural test bed requirement for wireless technologies at a global level, thereby making upcoming standards more inclusive and reflective of the circumstances in most countries; b) It reduces the potential capital expenditure cost for most telecom operators in the developing world as 5G will now be compatible with large cell legacy systems; c) It increases the coverage of 5G in the Indian rural areas.

fruition, as proposals in the pre-standardisation study are still to be formally accepted by the concerned departments. LITD 28 has also constituted a study group on 5G imperatives for Smart Infrastructure to define a smooth migration path from current frameworks and architectures to '5G inclusive' next generation homogeneous architectures[186].Further, consultations with stakeholders in LITD 28 revealed the presence of ongoing deliberations on development of an IoT reference architecture that adequately addressed national needs while conforming to global standards. Under this proposed unified reference architecture, the Communication Protocol Stack Architecture, Network Access Layer, a Common Services Layer and a Data Exchange Framework were being researched upon for their standardisation potentialities.

Additionally, TSDSI collects use cases for smart infrastructure and collaborates with stakeholders to harmonise standards in telecoms. The Ministry of Commerce (MoC) set up a High Level 5G Forums (HLF) to formulate a strategy for India to take lead on 5G[187]. TSDSI has published standard called CPRI Fronthaul Standard which specifies the functional block for front haul processing for transport of Common Public Radio Interface (CPRI) and/or GE from the Base Band Unit (BBU) or Radio Equipment Control (REC) to the Remote Radio Head (RRH) or Radio Equipment (RE) of a base station. More recently, it has submitted its IMT-2020 Radio Interface Technology (RIT) to the ITU-R which is currently under the scrutiny process. RIT is espoused by TSDSI to address the rural requirements of the Indian ecosphere by implementation of Low Mobility Large Cell (LMLC) which facilitates low-cost rural coverage of 5G, a technology integral to the success of IoT (Refer Box 1)[188]. Please refer to Figure 3.4 for a snapshot of SDOs and their standards across different component of a smart city ecosystem.

Figure 3.4: Standard bodies in India for Smart Cities



Source: *Compiled by authors*

India is also working closely with the Seconded European Standardisation Expert in India (SESEI) managed by ETSI and supported by EU organisations CEN and CENELEC, European Commission and European Free Trade Association (EFTA). The objective of the project is to promote alignment between both countries on production and use of ICT standards that could benefit European and Indian ICT standardisation efforts at the

186 *Ibid*

187 Making India 5G Ready. http://dot.gov.in/sites/default/files/5G%20Steering%20Committee%20report%20v%2026_0.pdf?download=1

188 https://techblog.comsoc.org/2019/07/05/indias-tsdsi-candidate-imt-2020-rit-with-low-mobility-large-cell-lmlc-for-rural-coverage-of-5g-services/

global level. ETSI and TSDSI, both oneM2M partner type 1, collaborate extensively on a series of standardisation subjects, especially in the domain of M2M and IoT. OneM2M is a global standards initiative that covers requirements, architecture, API specifications, security solutions and interoperability for machine-to-machine and IoT technologies. It is the software/middleware layer between applications and communication networking hardware/ software that is integrated into devices / gateways/ servers that enables storing and sharing of data. While most existing initiatives, protocols and standards go against the tenet of a unified and harmonized paradigm for smart infrastructure, oneM2M is considered to be one that is attempting to address the problem of unified architecture especially for complex use cases such as smart cities. Instead of a vertical approach, oneM2M enables different IoT use cases to be supported through a horizontal platform.

The use of oneM2M is slowly gaining popularity. South Korea operators including SK telecom, KT and LG U+ have rolled out oneM2M certified IoT platforms. OneM2M smart cities solutions have been used in the Korean city of Busan. In India, Tata Telecommunications is rolling out a huge LoRa (low-power-wide area network)supported by Hewlett Packard's (HP) oneM2M compatible platform[189]. HP's oneM2M platform has also been selected by the Bhopal Smart City Development Corporation Limited to created India's first cloud-based and integrated command and control center[190]. Since, HP has deployed its oneM2M platform across seven cities in MP. However, a study report by Confederation of Indian Industry (CII) titled "Study Report on "Information & Communication Technology (ICT) covering M2M/IoT and its Role in Smart City + Cyber Security" concludes that one M2M efforts are limited to the common service layer. The advantages of a platform such as oneM2M have been well established, especially in case of complex and large-scale implementations that require simultaneous coordination and data exchange across multiple device points. According to industry sources, the efficiencies of oneM2M kick in for a project with minimum 20000 devices. However, in case of smaller and less complex installation, onem2M may become overkill, given the costs associated with implementation of oneM2M. Accordingly, technology companies may use alternate platforms such as Trinity and Fluentgrid for aggregation and exchange of data in IoT system.

The discussions above find the role of standards to be paramount in the uptake of Industrial IoT, Consumer IoT and Smart Cities in India. The scaling of these technologies are however not limited to the development or availability of standards alone. For instance, the baggage of old machinery and huge costs associated with smart manufacture are limiting Industrial IoT in India. However, the growth of consumer IoT is mostly limited by the lack of security standards. Finally, the challenge with smart buildings and smart cities is the availability of affordable harmonized standards. Consensus building among stakeholders in the IoT ecosystem is a key requirement to speed up the standardisation process for smart cities. Moreover, the ecosystem must be dynamic to enable modifications and upgradations to current standards.

The next section presents a comparison of IoT policies across different countries and the role of national standard setting organisations. It also analyses the role of government and private players in enabling the IoT ecosystem in different countries.

3.5 Cross- Country Comparison: IoT Policies and Focus on Standards

[189] OneM2M White Paper "Smart Cities done Smarter ", Updated July 2018. http://www.onem2m.org/images/files/oneM2M_WhitePaper_SmartCitiesDoneSmarter.pdf

[190] CCDCSC will be a common platform where all the information from various sources like city operation centers and applications will be stored. All the information collected here, will be analyzed for better planning of the smart cities using integrated analytical layer / BI engine. These insights / trends will be helpful in managing incidents across the state and individual city and do a better planning for the development and delivery of smart city projects. The 07 cities selected/planned to be selected as part of Smart City Mission are as follows. Already Selected – Bhopal, Gwalior, Jabalpur, Indore, Ujjain, Satna and Sagar.

The successful deployment of IoT is contingent on both government and private sector led initiatives that provide an environment in which new technologies can emerge, flourish and grow. A cross-country comparison finds that governments in general have been slower than the private sector in responding to the IoT phenomenon. While there have been commitments from governments including Indutrie 4.0 in Germany, the Digital Single Market Strategy of Europe, the U.K Digital Strategy, the Smart Nation initiative of Singapore, the Digital India program, only a few countries have announced formalized policies. A comparison of available policies can help reassess India's existing approach and provide a reference to best practices.

3.5.1 India

In the case of India, two policies (in their draft versions) have been identified as pertinent to the development of IoT: a) IoT Policy Document released by the Ministry of Electronics and Information Technology (MeitY) and b) The Personal Data Protection Bill formulated by a committee lead by Justice BN Srikrishna. The IoT Policy Document explicitly states the intent of the Indian Government to harness the potential of IoT. IoT in this regard, is viewed as a policy enabler for two major initiatives of the Indian Government i.e. Smart City and Digital India Program[191]. The policy has identified a basic set of objectives which include: creating an IoT industry in India by 2020 (value of USD 15 billion); facilitating capacity development for IoT-specific skill-sets for domestic and international markets; promoting R&D for assisting technologies and developing IoT products in line with specific Indian needs in identified sectors[192]. To achieve these objectives, a five-pillar approach (namely *Demonstration centres, Capacity Building and Incubation, R&D and Innovation, Incentives and Engagement & Human Resource Development*) has been proposed with two horizontals (*Standards and Governance structure*) serving as the buttresses for the approach[193]. The undertone of the policy is holistic in the sense that the pillars can be viewed as long-term systemic changes rather than one-time institutional interventions. For instance, the policy's focus on reorienting degree programs in the light of emerging technologies under its *Human Resource Development* pillar clearly highlights the aforementioned notion.

From a standards perspective, the policy document recognizes the importance of standardisation (a horizontal in the policy's approach) and provides guidelines for promotion and adoption of the same in a separate section. In this section, directives have been offered for appointing a relevant nodal organisation (most probably BIS: Bureau of Indian Standards) in matters pertinent to IoT standardisation (like interoperability, technology stacking, reference architectures etc.). Furthermore, the creation of a National Expert Committee has been proposed and guidelines regarding its composition have been offered[194]. An overview of the technical committees of BIS currently deliberating upon standards for IoT (& other synonymous technologies) has been provided in the appendix 10.1.

The Personal Data Protection Bill[195] (draft) on the other hand, derives inspiration from its European counterpart, the General Data Protection Regulation (GDPR). The bill mainly seeks to a) provide strict guidelines regarding the processing of personal data by the government, domestic and foreign Companies; b) categorize data as: Personal Data, Sensitive Personal Data & Critical Personal Data; c) state the rights of citizens in context of their data[196]. If passed, it becomes crucial in the context of IoT, especially consumer IoT, since there remain ambiguities with respect to the secure processing of data in M2M data transactions.

---

191 IoT Policy Document. https://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf

192 Ibid

193 Ibid

194 Ibid

195 The Personnel Data Protection Bill 2018. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

196 Cisomag (2020). "All You Need to Know About India's First Data Protection Bill", Cisomag, January 3, 2020. https://www.cisomag.com/all-you-need-to-know-about-indias-first-data-protection-bill/

3.5.2 Singapore

Though there is an absence of an exclusive IoT policy in Singapore, it's fragmented (in the sense that it is carried out by different government agencies) development and standardisation efforts unify to achieve the ends of its comprehensive Smart City policy i.e. Smart Nation Initiative launched in 2014. According to some policy commentators, it was ideated mainly to achieve two broad objectives i.e. *improving people's lives* and *creating more opportunities*[197]. It is imperative to note here that Singapore enjoys a massive advantage as a vanguard of disruptive technological adoption due to its rich human (knowledge economy) and infrastructure resources[198]. The language of the policy is very people-centric and inclusive in the sense that guidelines provide directions for all stakeholders. The Smart Nation Initiative aims to bring about transformation in five key domains: *Health, Transport, Urban Solutions, Finance and Education* via three schemes: Digital Economy, Digital Government Blueprint and Digital Readiness Blueprint[199].

It is apparent that IoT is a central policy enabler for the Smart Nation Initiative. The policy recognizes the vulnerabilities posed by IoT proliferation and aims to preclude them with the help of a strong system foundation. In the language of the policy, systems foundation refers to reengineering of technological infrastructure in the fields of *cybersecurity, data value maximization and digital infrastructure*[200]. For notable legislations, kindly refer to the *Appendix10.2*

From a standards perspective, five TRs[201] (Technical References) and a cybersecurity guide have been developed by the IMDA (Infocomm Media Development Authority; IDA is the more common abbreviation) and ITSC's IoT Technical Committee (Information Technology Standards Committee)[202]. The justification provided by IMDA for promulgation of such standards is the absence of a blueprint which connects the innumerable IoT standards available to form a conducive ecosystem of inter-operable sensor network devices and systems[203]. As indicated by Singapore's Minister of Foreign Affairs, Dr. Vivian Balakrishnan, the nation's IoT strategy revolves around open standards[204] (to preclude vendor lock-ins). This intent manifested itself with SSIA's (Singapore Semiconductor Industry Association) collaboration with OCF(Open Connectivity Foundation) to promote an open standard specification for SMEs in Singapore[205]. The collaboration can be viewed as the perfect example of government-private sector collaboration in a time where one sees government policies lagging behind private efforts. Furthermore, IDA is also conducting a trial for its new OTA SM[206] (Over-The-Air Subscription Management Standard) standard with different mobile network operators[207]. The participation of mobile network

[197] Woo, J. J. (2017). Singapore's Smart Nation Initiative–A Policy and Organisational Perspective. *Lee Kuan Yew School of Public Policy, National University of Singapore*.

[198] Smart Nation Initiative Policy Doc

[199] Smart Nation Initiative Policy Doc

[200] Ibid

[201] A Technical Reference is a pre-Singapore Standard (SS) that is designed to meet an urgent industry need. It is directly implemented without a two-month public review to preclude the possibility of being outmoded while it has been released. After two years of its implementation, feedback is derived from the industry on its use and a review is made on its suitability. Based on the review's nature, the TR may be subjected to a) further industry trial; b) withdrawal of TR; or c) Elevation to a SS (Singapore Standard)

[202] Detailed Overview provided in appendix

[203] https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Internet-of-Things

[204] Tan. A (2018). "Singapore government outlines its approach to IoT", computerWeekly.com, March 21, 2018. https://www.computerweekly.com/news/252437239/Singapore-government-outlines-its-approach-to-IoT

[205] Open Connectivity Foundation and Singapore Semiconductor Industry Association Announce Collaboration Framework in Singapore, March 28, 2017. https://www.businesswire.com/news/home/20170328006371/en/Open-Connectivity-Foundation-Singapore-Semiconductor-Industry-Association

[206] This is of paramount importance for IoT as most embedded SIMS on IoT devices cannot switch between different mobile network operators.

[207] https://www.imda.gov.sg/news-and-events/impact-news/2016/01/leading-the-charge-for-open-iot-standards

industry players in the trial will have a significant impact on the development of this standard and possesses the potential to reduce the government industry intervention gap.

3.5.3 Germany

While Germany does not have a comprehensive policy dedicated to IoT, it is enabled through its policies on Industrie 4.0 (I4.0). I4.0 was initially conceived to preserve Germany's status as a market leader in the manufacturing sector driven through a slew of policy initiatives namely *High Tech Strategy (2006), Deutschland Digital 2015 (2010), High-Tech Strategy 2020 (2010), Action Plan HTS 2020 (2012), Digitale Agenda 2014-2017 (2014) and HTS Update (2014)*[208]. The focus of these policies began as parochial, largely limited to the Industrial Internet of Things (IIoT). Over years it has expanded to include other IoT applications. Emphasis on standardisation is visible in the language of certain policies. In *Deutschland Digital 2015 (2010),* a project for future I4.0 focuses on the development of open standards and interoperability while another encourages the augmentation of R&D specifically in IoT[209]. *High-Tech Strategy 2020 (2010)* proposed an inclusive National Roadmap for IoT making standardisation a normative aspect of R&D to ease transition to market[210]. One of the working groups under *Plattform Industrie 4.0" (PI4.0)* (which was initially an industry-led initiative[211]) focused exclusively on *reference architecture, standardisation and norming*[212]. A tangible effort in this direction is the release of the *Reference Architectural Model for Industrie 4.0* (colloquially known as RAMI 4.0), a model designed to give companies a common framework for developing future products and business models[213]. *Plattform Industrie 4.0* also facilitates co-ordination with the Standardisation Council Industrie 4.0, a body responsible for initiation of cross-sectional standards, co-ordination of national and international standards and strengthening German-international co-operations[214].

3.5.4 United Kingdom

Two policies are found to be germane to IoT in the UK i.e. UK Digital Strategy and Secure by Design report. The two policies differ scale and focus areas. The UK Digital Strategy outlines the vision and intent of the UK government to digitalise its fundamental economic structure via seven strands i.e. *Building world-class digital infrastructure for the UK, giving everyone access to digital skills they need, making UK conducive to start and grow a digital business, helping every business become a digital business, making the UK the safest place in the world to live and work online, maintaining the UK government as a world leader in serving its citizens online and unlocking the power of data in the UK economy and improving public confidence in its use*[215]. While this is not an IoT specific policy, it is commonplace to assume IoT as a policy enabler. Moreover, the policy also directs an increase in IoT research. To instill public confidence and drive the adoption of IoT, the policy also states the role of the EU General Data Protection Regulation (GDPR), which is crucial in the context of M2M communications for IoT.

On the other hand, the UK's Secure By Design Report is an IoT specific policy that focuses on implementing a code of practice for all IoT manufacturers (producing consumer IoT products)[216]. Focused on consumer security, it outlines a basic set of guidelines to eradicate rudimentary security loopholes that might be exploited (To preclude

---

208 UNIDO Report: What can policymakers learn from Germany's Industrie 4.0 Development Strategy

209 Ibid

210 Ibid

211 The German government was hesitant to join initially, but as this gained more traction, a lot of players wanted to join. Even though the government collaborated, it was mainly run by business corporations with the government playing an advisory role.

212 Ibid

213 RAMI 4.0Reference Architectural Model for Industrie 4.0 https://www.isa.org/intech/20190405/

214 Industrie 4.0 Standardization in Germany Dr. Bernhard Thies. http://www.miit.gov.cn/n973401/n4965332/n5406930/c5448374/part/5448401.pdf

215 https://www.gov.uk/government/publications/uk-digital-strategy/executive-summary

216 https://www.gov.uk/government/collections/secure-by-design#history

botnet attacks like the Mirai malware)[217]. Currently, deliberations are going on around the question of mandating such guidelines.

However, the BSI group (a non-profit) is way ahead of governmental interventions in offering standards compliant solutions for various stakeholders (like manufacturers, discrete government agencies etc.) in the IoT ecosystem. This is conspicuous in its Testing and Certification scheme for IoT devices which are divided into three phases: (1). IoT Device Testing; (2). IoT device verification; (3.) BSI Kitemark IoT Device Certification[218]. Such a service helps numerous vendors navigate through the complex standards landscape (a problem previously discussed in Chapter 2 and isn't comprehensively addressed by government policies). BSI has also developed the PAS 212:2016 standard: Automatic resource discovery for the Internet of Things specification[219]. Another industry-led specification is Hypercat, a technical specification for IoT developed by Hypercat (a consortium led by approximately 40 UK based companies) which eases communication amongst discrete IoT devices[220]. The specification isn't a standard yet, but represents the industry's cognisance to minimise chokepoints for the complete realisation of IoT

3.5.6 EU and the United States

EU's efforts towards IoT seem to coalesce under the policy direction of the Digital Market Strategy. It is cited to resolve bottlenecks of data flow across various IoT devices and platforms in the EU bloc[221]. This strategy also led to the inception of the Alliance for Internet of Things Innovation (AIOTI), a body that aims to strengthen the dialogue and interaction amongst Internet of Things players in Europe[222]. It consists of 13 Working Groups (WG) (*details in Appendix10.3*), out of which WG 03 works exclusively on IoT Standardisation. Furthermore, regulations like *Regulation on the free-flow of non-personal data* aim to preclude data localisation to expedite the IoT's potential realization and the services contingent on it[223]. The GDPR is another landmark legislation which concerns protection of data. From IoT's perspective, few technical issues arise with the GDPR's simple consent mechanism which policymakers have tried to address to a certain degree[224]. Another security standardisation effort that is worth noting is the release of the ETSI TS 103645 standard, which provides a security baseline for web-connected devices while simultaneously proposing plans for future IoT certification plans[225]. ENISA (European Union Agency for Cybersecurity) has also released recommendations in a publication titled *Securing Europe's IoT Devices and Services*[226]. Other EU IoT regulations are briefly mentioned in Appendix 9.3

In the United States, standardisation efforts are led by the National Institute of Standards and Technology (NIST). The IoT Cybersecurity Policy released in 2017 in collaboration with the US Chamber of Commerce underscored the importance of security in realising IoT's full potential and briefly mentioned NIST's Industry lead *Framework for Improving Critical Infrastructure Cybersecurity*[227]. California's SB-327 law is a state law which addresses IoT security. The law mandates IoT manufacturers to equip their devices with 'reasonable' (no clear explication provided for

---

217 https://duo.com/decipher/uk-government-proposes-secure-by-design-guidelines-for-iot
218 https://www.bsigroup.com/en-GB/industries-and-sectors/internet-of-things/IoT-Assurance-Services/
219 https://shop.bsigroup.com/forms/PASs/PAS-212-2016-download/?_ga=2.233330650.533840632.1578894669-1576217135.1578894667
220 https://www.techradar.com/news/internet/web/what-is-hypercat-exploring-the-latest-internet-of-things-standard-1255230
221 https://ec.europa.eu/digital-single-market/en/internet-of-things
222 https://aioti.eu
223 https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data
224 https://www.i-scoop.eu/internet-of-things-guide/iot-regulation/#IoT_and_Data_Protection_Impact_Assessments_under_the_GDPR
225 https://analyticsindiamag.com/iot-security-standards-hackers/
226 https://www.enisa.europa.eu/events/copy_of_enisa-workshop-on-cyber-security-for-iot-in-smart-home-environments/1-enisa-securing-europes-iot-devices-and-services/view
227 https://www.nist.gov/system/files/documents/2017/10/23/mattheweggers_slides.pdf

what constitutes reasonable) security features[228]. Apart from this, it is observed that there is no policy on federal level that acts as a peer to EU's GDPR.

It becomes important to note that in the case of both the EU and the US, there have been significant contributions from the private sector towards harmonisation of IoT. The most notable effort includes the promulgation of multi-layer frameworks by different consortia and companies based in these two regions. Examples include open source stacks like IoTivity (led by Intel and Samsung Electronics), OpenWeave (created by Google) and Homekit (developed by Apple)[229]. Though these aren't encompassing umbrella frameworks, they have reduced fragmentation in the ecosphere to a significant extent. Furthermore, companies like Cisco, HP, Intel, Vodafone etc. regularly release white papers and reports summarizing the current IoT landscape whilst also providing policy recommendations and guidelines to all stakeholders. It is also to commonplace to forget that most of the international industry consortiums are comprised of such companies.

After this brief overview, one finds that even though certain countries like the United States lack a comprehensive national IoT policy, their ecosphere seems to be more mature. This could be ascribed to two main reasons: a) most of the technological breakthroughs occur in these countries which also happen to possess strong existing infrastructure; b) increased cognizance of the importance of standards amongst the private sector (manifest in the presence of consortiums). The interaction of these two elements in a laissez-faire manner makes it easy for other countries to guide the standardisation efforts via different policies, thereby giving IoT innovation a guise of structure. This, however, does not eliminate the role of the government, which must constantly monitor businesses to protect consumers from abuse of dominance and risks to national security.

India, despite the presence of a comprehensive IoT policy, has seen limited and very recent progress in standardisation. As mentioned in previous chapters, standardisation efforts in India are led by a handful of companies, mostly of foreign origin. This implies the absence of a strong standardisation 'culture' within the domestic private sector (which itself is fragmented due to a mixed composition of start-ups and established technological corporations). Though this is changing, the process of change is labored. It thus becomes imperative that there exists a healthy balance between government policy and the Indian private sector so that such a culture can be engendered, and the India transcends the nascent stages of IoT.

4. Recommendations and Conclusions

IoT has ushered India into its next phase of technological revolution. However, the unequivocal acceptance of value that this technology can bring to businesses and societies is challenged by the exponential rise in the number and types of devices that pose serious regulatory concerns. Adoption of standards is not only central to driving the commercial viability of IoT products and services, but standardized quality and security assurance also help IoT applications reach their full potential. Standards enable economies of scale and scope, reduce transaction costs and avoid duplication of efforts, especially for new entrants. It also establishes trust within the user community. Standardisation in IoT will enable data exchange through interoperable components and software, establishing network externalities[230]. However, standards have to be upgraded and continuously adjusted to technical progress, often resulting in moving targets for interoperability. It is a knowledge intensive activity demanding the involvement of multiple stakeholders. Policy prioritization and fiscal support can become very important to keep the standards ecosystem alive.

228 https://www.thesunflowerlab.com/blog/what-is-california-iot-law-or-sb-327/
229 https://www.leverege.com/blogpost/iot-standards-and-protocols
230 Katz. M and C. Shapiro. 1985. "Network Externalities, Competition and Compatibility. "American Economic Review "75 (3):424-40

India is a latecomer to standard setting for IoT. U.S, Germany, Japan and Russia have enjoyed first mover advantages in standard setting. Setting up of TSDSI was a significant milestone for India. It created an ecosystem that works towards developing and promoting India–specific requirements for IoT. India also has the advantage of borrowing and adapting existing standards and technology. In the globalized market for IoT, isolating India would only mean limiting the scale and scope of developing this technology. Government must step up its role in facilitating the development and adoption of standards. India needs to put efforts both in standards development and adoption. Below are some policy recommendations on standards development (upstream) and standards adoption (downstream) in India, both at critically low levels about IoT and related technologies.

4.1 Encourage Centralised and Co-ordinated Development

The current process of standards development and adoption in India appear ad hoc. Stakeholders including SDOs need to identify national priorities and map the requirements to stakeholders, across government, private players and non-government organisations. There is absence of a comprehensive framework that articulates and prioritizes standardisation activity across SDOs. Inter-ministerial deliberations are a pre-requisite for policy making in cross-cutting sectors such as IoT. Simultaneously, collaboration between BIS, TEC and TSDSI is important to develop IoT standards that collectivity address the needs for security, identity and interoperability. An effort to work with technical committees has seen limited success (Work held up in the BIS Committees on Standards for Smart Infrastructure). However, such member-initiated discussions followed by white papers and proposal for research projects, test beds, pilot's etc. do help in better understanding of India specific use cases.

The multitude of IoT verticals leads to the creation of silos which precludes the congregation of rich data sets collected by vendors of each vertical and can sometimes lead to a duplication of standardisation work amongst different SDOs. In the context of smart cities, this becomes exigent since aggregation of these data sets can lead to better governance mechanisms while streamlined standardisation research can mitigate the time and utility cost of duplication. Further, collaboration and adoption of common reference architecture for smart cities mitigates the problem of vendor lock-in, a phenomenon that is more conspicuous in the consumer IoT space. If collaboration isn't pursued as a value-goal, it defeats the inherent purpose of deploying IoT in Smart Cities as these solutions were deployed to enhance the existing city governance mechanisms (not convolute them).

A coordinating agency must be designated the task of harmonizing the standardisation needs across various verticals and simultaneously work on strengthening the horizontal platform.

4.2 Invest in Research& Development

The importance of research and innovation cannot be overstated for development of standards. At present India's collective R&D spending as a percentage of GDP is only 0.8 percent.[231]Standard driven innovation and research can play a critical role in adoption and scaling of new technologies. Moreover, all emerging technologies including IoT, AI, VR/AR are developing simultaneously and their combinations as illustrated in the sections above are evolving rapidly. Research and development in these areas will continue alongside product development.

For IoT, funding support, both from the government and the private sector will be critical in developing capabilities in 5G, smart cities, technology interoperability and security. Private sector initiatives in this direction are very encouraging. Unlimit, an end-to-end IoT service provider in India, has opened its new R&D Centre in Bengaluru. Their focus is on customised projects, supply chain, connected vehicles and industry 4.0. NASSCOM's CoE-IoT established the largest eco-system for deep tech product innovation. There are over 40 start-ups, employing over 250 innovators that are building products & solutions in healthcare, sports, domestic appliances, industrial safety, etc.

---

231 http://uis.unesco.org/apps/visualisations/research-and-development-spending/

One government led initiative is "IoT Open Lab" – a centre of excellence (CoE) in Bengaluru launched by the Software Technology Parks of India (STPI). The IoT Open Lab uses a collaborative model to nurture startups and drive R&D, innovation and product development for sectors like defence, aeronautics, industrial, agriculture, health, automotive and education. The Lab has also established academic partnerships with engineering colleges.

In Europe and USA, IoT markets have been steered by the private sector with the government overseeing regulations. Government funding has been provided to special projects such as smart metering in the USA. These are targeted funding opportunities and not ones that look at expanding the IoT market overall. The governments are also neutral on the choice of technology. The Chinese government, on the other hand, has played an instrumental role in supporting the development of technology and new markets for IoT. China's Ministry of Industry and Information Technology in its 12th Five-Year Development Plan (2012), announced to spend 1,000 billion ($163 billion) by 2020 to scale up the IoT market. At the same time, the government's IoT Special Fund is promoting IoT research and development, applications and services. Grants are offered to self-funded projects, and loan subsidies support enterprises with bank-loan funding. India can work with either alternatives or a middle path that enables the private sector while supporting key government-led development initiatives. The government must however focus on building skill sets necessary for IoT research. This implies strengthening the educational curriculum around IoT including certification courses, exchange programs, trainings, etc.

4.3 Strengthen Governance of Indian Standards Bodies

Since India has recently embarked on standardisation activities for IoT, an assessment of the functioning and governance mechanisms including membership fees, policies, norms, guidelines and good practices, policies on IPRs etc. of various SDOs in India would be a good starting point to check against anti-competitive outcomes and achieve objectives of maximum participation, speed of standard adoption, etc. A good governance system should also check SSOs that deliberately exclude rivals, offer members a significant market advantage, etc. Analysing these factors could provide a useful guide for India to improve upon the quality of their SDOs and encourage greater participation of its members in the domestic and global standards development process.

4.4 Integrate MSMEs and Start-ups

Historical trends suggest that many MNCs invest in technology research. Accordingly, standard development and adoption is driven by big companies or consortia led by them. More recently, research has become localised, startups and academic institutions are working independently as well as collaboratively on new products and services. There is a stronger recognition of standardisation efforts being made by MSMEs. Larger MNCs are now looking at MSMEs to provide some key differentiators in their product lines. MNCs also fund startups and MSMEs that are very agile and well suited for niche cutting edge problem solving. Some successful examples of MSMEs and individuals participating in the standardisation process are summarised in Box 3 below.

AstraZeneca's BioVenture Hub is a great example of cultivating a culture of collaborative innovation integrating MSME, startups and academicians. The Hub provides a unique opportunity for smaller companies and innovators to interact with big companies to advance technology. Inviting MSMEs and startups along with big trend setting companies to industrial parks and offering them free access to new standards and technology will encourage its wide scale adoption among MSMEs. Both standards development and adoption are expensive propositions and MSMEs as well as startups need to be hand-led both technologically as well as financially to encourage adoption of new standards. This triple helix approach, popular in many countries can become the way forward for India.

Box 2: Examples of Individuals and MSMEs from India who have successfully participated in the Global Standardisation Process

1. The IEEE P1931.1 is an IoT Standard for providing Real-time Onsite Operations Facilitation (ROOF). ROOF computing and networking for data and devices includes next-hop connectivity for devices, real-time context building and decision triggers, efficient backhaul connectivity to the cloud, and security & privacy. This standard defines how an end user is able to securely provision, commission and decommission devices. It leverages existing applicable standards and is complimentary to architectural frameworks defined in broader IoT environments.

   The standard was proposed by Mr. Syam Madanapalli, in his individual capacity to the IEEE Communications Society in 2016. IEEE approved the project authorisation request for active work on the IEEE P1931.1 standard. The project participants included representatives from both India and outside. All relevant stakeholders including consumers, device manufacturers, solution providers, service providers, utilities, governments, ICT infrastructure providers, ISPs and vertical enterprises were made a part of the process. One of the start-up participants from India included Mr. Nishant Krishna from Tech Machinery Labs. IEEE P1931.1 is still to be published. BIS is yet to confirm if they will adopt the standard once it is published.

2. IEEE 802.15.4™ is a global standard for developers of smart city and Internet of Things (IoT) applications. IEEE 802.15.4 was developed to enable low-data-rate applications that require years of battery life, low-complexity architectures to minimize cost and the ability to operate in unlicensed spectrum. Examples include smart utility grids, street light management, building automation, home control and residential security.

   IEEE 802.15.4u™ is the first standard to support the 865-867 MHz band for applications in India, completely complying with the country's wireless regulations. Amarjeet Kumar. CTO & Managing Director of Procubed Technology Solutions proposed this amendment to the IEEE 802 standards committee. He has been an active contributor in the development of communications standards and the specification of test plans for a number of Smart Utility Network standards. The addition of IEEE 802.15.4u™ benefits developers, service providers and end users by providing them an alternative to proprietary implementation in the 865-867 MHz band. As a result, they can now choose from a wider selection of IEEE 802.15.4-based solutions providers with greater independence and multi-vendor interoperability. This compatibility also creates additional opportunities for Indian IoT and smart city applications to leverage IEEE 802.15.4's global ecosystem and marketplace momentum. For example, IEEE 802.15.4u replicates IEEE 802.15.4g's radio frequency (RF) characteristics into the new sub-GHz band defined for India.

4.5 Enhance Participation in Global Platforms

A unanimous response from stakeholders suggests that India's biggest disadvantage is its underrepresentation in global standards fora including ITU-R, 3GPP, One M2M, ITU-T etc. As highlighted above, representatives from India are changed periodically, resulting in discontinuous engagements and poor outcomes. This concern needs immediate redressal for India to gain traction in the global standardisation process and exercise voting rights for adoption of a standard by stating domestic preferences. Participation in these meetings are important both for standards development as well as adoption. Countries like China, Korea and Japan are active participants and are well represented with delegation strength of 20-50 people making significant contributions at these forums. India on the other hand is not only underrepresented but the nature of participation is inconsistent. The limited participation from India has created a perception amongst the global community of India lacking understanding on standards. Further, participation from education institutions in some of the forums has changed only moderately as academicians perceives standards curtail innovation. The trends of participation over the years have only observed significant improvement. For instance, 100 participants from India represented in IETF in 2015 which has only increased to 120-140 in 2020.Please refer to Box 3 for TSDSI's recommendation on improving standardization efforts through improved participation in global fora.

Box 3: TSDSI Recommendations and Strategy for Improving India's Participation in Global Fora

1) Create a pool of standardisation experts: Nurture a team of about 50 experts with diverse skills representing academia, government labs and start-ups
   - Need consistent participation over 5-10 years to build global leaders
   - Strategically target meetings for high impact contribution related to national priorities
     - 10-3GPP
     - 5- ITU-R and 5 -ITU-T
     - 5- One M2M
   - Delegation size of 5-10 members each
   - Attending these meetings costs almost INR 7 crores every year[1] and therefore fund allocation for travel is critical.
   - Key criteria for delegation selection
     - Technical contribution and participation in TSDSI SG/ WGs
     - Only India centric organisation represented in India delegation
2) Bring more meetings of global platforms to India for enhanced domestic participation. A strategy is needed to streamline this. The specific challenge of getting MEA/MHA approvals to enable visa and travel arrangements for global experts is becoming a bottleneck and needs government support.

3) Enhancing influence through Local and Regional Alignments to become more effective. This could be achieved by:

- Participating in Regional forums like ITU-RG, APT, CJIK; championing Standards lifecycle activities in SAARC, APAC region.
- Collaborating with other Industry bodies – COAI, IEEE- India, BIS etc. Partner flagship national events like IMC, M2MIoTForum, 5GIA etc.

4) Capacity Building: Formal Training programs on how to become effective in Standards fora; Quality Audits of TSDSI

4.6 Build Awareness among the Developer Communities

At present the stakeholders including academia, industry, startups etc. lack awareness on the standards and the standard development process. Organising hackathons is a good way to create awareness among developers and encourage them to develop utilities, ideas, sample code and solutions using standards. Further webinars can also act as a medium to educate the technologists and other stakeholders about standards.

4.7 Encourage IoT Consultancy and Certification Services

The multiplicity of products and standards can lead to a choice paralysis for end users (such as vendors and different corporations) and may result in sub-optimal choices led by cheaper but poorer technologies. The BSI's (British Standards Institute) testing and certification for connected IoT devices helps new manufacturers gain market acceptance. Comprehensive consultancy services (which can be availed by companies of varying scales i.e. from startups to established MNCs) will create a culture of standardisation among end-users which as a consequence, will also augment trust amongst users and expedite growth. When established through a public – private partnership model such bodies serve two important utilities: a) it reduces the informational asymmetry regarding established standards for all stakeholders (most importantly for new SMSEs and startups); b) It becomes the nodal agency for ensuring implementation of India specific standards. In the long run it will also push consumers to become conscious consumers, investing in safety and quality assurance of the products they purchase.

4.8 Focus on Standards for Smart Cities

The discussions in Chapter 3 establish the essentiality of interoperable systems in smart city deployments. Adherence to internationally agreed standards including technical specifications and classifications enables a larger pool of vendors to integrate into the ecosphere. NASSCOM and Accenture's report titled "Integrated ICT and Geospatial Technologies Framework for 100 Smart Cities Mission" has listed down 55 global standards keeping in view several city sub-systems that could be applied to the Smart Cities in India[232]. Bureau of Indian Standards has set up technical committee to formulate standardized guidelines for central and state authorities' in planning, design and construction of smart cities. Developing national standards on Smart Cities in line with existing international norms. The current framework lets cost concerns over ride issues of quality and interoperability. To maximize participation and address issues pertaining to data protection, privacy and other risks associated with smart cities developing standards for smart cities is essential.

At present, there is limited interoperability and ecosystem is locked in by bigger vendors. The technology trends in "Smart Homes", "Smart Building", "Smart Grid", "Smart Water", "Smart Transport" and "Smart Cities" are deployed in silos leading to inefficiencies. For interoperability, harmonization of standards is critical. There is need for a common framework and defined architecture for the software, hardware and network infrastructure to be deployed. Since data is crucial for smart cities, a comprehensive data management standard in India will enable quick scaling and instill public confidence and trust.

While the multitude of IoT verticals in the space offers a range of choices to the end user/government, it leads to the creation of silos which precludes the congregation of rich data sets collected by vendors of each vertical and can sometimes lead to a duplication of standardisation work amongst different SDOs. In the context of smart cities, this becomes exigent since aggregation of these data sets can lead to better governance mechanisms while streamlined standardisation research can mitigate the time and utility cost of duplication. Further, collaboration and adoption of common reference architecture for smart cities mitigates the problem of vendor lock-in, a phenomenon that is more conspicuous in the consumer IoT space. If collaboration isn't pursued as a value-goal, it defeats the inherent purpose of deploying IoT in Smart Cities as these solutions were deployed to enhance the existing city governance mechanisms (not convolute them). This has been corroborated by AIOTI's 'High Priority IoT Standardisation Gaps and Relevant SDOs' Report 2020 which stresses on the need for mapping standards to their vertical legacy systems so that only the appropriate SDO pursues research to address that area. An example of standard duplication has been provided in the field of Agricultural Machinery, wherein the integration of new features involving the triggering of mechanical movements falls under the purview of more than one SDO[233]. AIOTI's report cites the multiplicity of heterogeneous and competing standards and/or protocols in the following domains: a) Connectivity (Various communication and networking technologies); b) Integration/Interoperability (Competitive platforms); c) IoT Architecture [Multiple High-Level Architectures (HLAs)].

Standards National Action Plan (SNAP) 2019[234] from BIS seeks to mitigate this problem by facilitating the creation of standardisation cells. These cells seek to cultivate both awareness and participation of stakeholders in

---

232 See: http://www.nasscom.in/integrated-ict-and-geospatial-technologies-framework-100-smart-cities-mission.

233 https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

234 SNAP has been accorded a priority score of 1.60[234] (Scale ranges from 3.20 to 1.00) based on the national socio-economic requirements. The score predicated on these requirements was determined via the collation of data in two areas: a) Analysis of GDP and trade contribution of different sectors based on the datasets of Balance of Payments (Ministry of Commerce and Industry), Export-Import (Department of Commerce) and National Account Statistics, 2017; b) Secondary analysis of NITI Aayog Reports, three-year action plans, policy postures of different ministries, Indian developmental programs and Reports by International bodies. When juxtaposed with other traditional sectors like Electronics (2.00)&New and Renewable Energy (2.20) and a few service sectors like E-Commerce (2.00), Legal Services (2.00) and Transport and Logistics (2.60), it is observed that the area of Digital Technologies is afforded a higher priority. This can partly be explained by the centrality of these technologies as policy instruments for the Indian

the standardisation process via the means of collaboration, inclusion and periodic consultations with government bodies, academia, other SDOs, regulators, Industry associations and discrete industrial entities. As of 24th June, 2020, no standardisation cells are visible on the BIS website. The historicity of various news reports seems to indicate the general lack of coordination on an inter-ministerial level as well the centre and other private entities. Nonetheless, to ensure smooth harmonisation of standards, it plans to extend the scheme for accreditation of SDOs (granted under the Section 10 (2) (c) of the BIS Act 2016 and Section 30 of the BIS Rules, 2018) whilst simultaneously conducting training on good standardisation practices for other SDOs in India[235].

4.9 Focus on Standards for Cyber-Security Governance

The recent SANS report[236] on securing industrial control systems (ICS) 2017, discusses cyber risks for industrial IoT in India. The top three threat vectors in ICS are: (i) 44% devices and "things" cannot protect themselves, (ii) 43% are accidental internal threats, and (iii) 40 % are prone to external threats from hacktivists or nation-states. To address the security and privacy challenges Indian government has introduced various policies including (i) Draft Indian IoT Policy, 2015, (ii) the personal data protection bill 2018 (iii) the cyber security strategy 2013 (iv) the 12th plan of cyber security 2018 and (v) the National Digital Communication policy 2018.

The present IoT policy encourages public-private partnerships (PPP) to secure critical infrastructure in the IoT domains. However, the implementation is not full proof. The government's top down approach is[237] hindering coordination and cooperation between various parties. The Indian IoT solutions especially IIoT is in dire need of a standard to reduce security risks which currently lacks implementable reference architecture.

The lack of trust in devices is also limiting the adoption of Consumer IoT. IoT devices increase the number of entry points into a home and the rapid manufacture of new devices exacerbates the risk of cyber-attacks. A key focus area for IoT standards in India should be securing the ecosystem and all interconnected devices.

Government's Smart City and Digital India initiatives. Further, SNAP states policy objectives to achieve harmonisation of standards and increase India's standardisation clout in strategic sectors at technical committees of different International SDOs

235 As per existing documentation on the BIS website, the following bodies are recognised as SDOs: a) e-Governance Standards Portal (Department of Information Technology); b) Standardisation Testing and Quality Certification (Department of Information Technology) and c) Telecommunications Engineering Centre (TEC under DoT).

236 Gregory-Brown, Bengt. "Securing Industrial Control Systems-2017." A SANS Survey. SANS Institute (2017)

237 Muppiri. C (2019). "Public-Private Partnerships in Indian Industrial IoT A Set of Policy Recommendations to Improve Cyber Security", Cybersecurity Academy. https://d1rkab7tlqy5f1.cloudfront.net/TBM/Over%20faculteit/Afdelingen/Engineering%20Systems%20and%20Services/People/Professors%20emeriti/Jan%20van%20den%20Berg/MasterPhdThesis/PPP%20in%20Indian%20IIoT_Chandra_Thesis%20%20Final.pdf

5. List of Stakeholder Consultations

We organised stakeholder consultations and meetings with sector experts, standard setting organisations, IoT companies as well as startups for a better understanding of the ecosystem. The list of stakeholders consulted for the study is summarized in table below.

Table 5.1 List of Stakeholders Consulted

Name			Organisation
Ms.	Bindoo	Srivastava	TSDSI
Ms.	Pamela	Kumar	TSDSI
Mr.	Sri	Chandra	IEEE
Mr.	Jitender	Kumar	BIS
Mr.	Dinesh	Sharma	Director, Standards Public Policy, EU Project SESEI
Mr.	R.	Pathak	DoT
Mr.	Satyan	Gupta	ITU, APT foundation of India
Mr.	Manoj	Misra	Sr. Public Policy Director –India, GSMA
Mr.	PVG	Menon	President & CEO, VANN Consulting Pvt. Ltd.
Mr.	Kishor	Narang	Narnix
Mr.	Aurindum		CDOT
Mr.	Sunil	Abraham	CIS
Mr.	Sudhanshu	Mittal	Centre of Excellence
Mr.	Sumeet	Swarup	NASSCOM
Mr.	Nishant	Krishna	HP – Bhopal Smart City
Mr.	Debashish	Dutta	HP – Bhopal Smart City
Mr.	Bipin	Kumar	Gaia Smart City
Ms.	Keerthi	Lal	India Electronic and Semiconductor Association
Dr.	Indrajeet	Bhattacharya	National Accreditation Board for Education and Training
Mr.	Shivaram	PV	B&R Industrial Automation
Mr.	Ashutosh	Chincholikar	Smart Controls India Ltd
Ms.	Sujata	Tilak	Ascent Intellimation
Mr.	Vivek	Shivaswamy	Samsung - OCF
Mr.	Nikhil	Kaura	Samsung
Mr.	Deepak	Maheshwari	Symantec
Mr.	Sharad	Arora	Sensorise

6. Sanction orders, Minutes of 1st and 2nd PGRC meeting, SEUC's

6.1 Approved Minutes of the First PGRC Meeting

Minutes of the Project Guidance & Review Committee (PGRC) meeting for the study titled **"The Role of Standards in Diffusion of Emerging Technologies: Internet of Things (IoT)"** by **Indian Council for Research on International Economic Relations (ICRIER), New Delhi** under A2K+ Studies, program of DSIR.

Date: 22-05-2020 Venue: Video Conferencing, Cisco-Webex.

Participants:

PGRC:

1. Prof. Sanjiva Prasad, Professor, IIT Delhi,	Chairman
2: Sh. Ashwani Gupta, Scientist G & Head A2K+ Studies, DSIR	Co-Chairman
3: Dr. Jitendra Kumar, Scientist D, Bureau of Indian Standards, New Delhi	Member
4. Dr. Suman Mazumdar, Scientist D, DSIR	Member Secretary

Others:

5.	Dr. Vipin C Shukla, Scientist F, DSIR	-
6.	Dr. Kailash Petkar, Scientist C, DSIR	-

ICRIER, New Delhi.

7.	Ms. Mansi Kedia	Principal Investigator (PI)
8.	Sh. Tanay	
9.	Sh. Rohit.	
10.	Dr. Rajat Kathuria, Director General.	

1. Dr. Kavita Bhatia, Scientist G, MeitY could not attend the meeting due to her prior commitments. Through video-conferencing, Co-Chairman of PGRC welcomed the Chairman, committee members, Principal investigator and her team members and Director General ICRIER, New Delhi to this meeting. Co-Chairman briefly explained the terms & conditions under which this Study was sanctioned by DSIR. He also briefed the terms of reference of this PGRC in relation to the acceptance of the submitted study report. Co-Chairman latter requested Prof. Sanjiva Prasad, Chairman PGRC to conduct the meeting. Chairman greeted the members and PI and her

colleagues from ICRIER, New Delhi and invited Ms. Mansi Kedia to make a presentation and brief the committee regarding final outcomes from the study.

2. The broad objective of the study was to (i) understand the role of standard-setting organizations (SSO) and the industry in setting & conforming to standards; (ii) explore characteristics of an efficient 'architecture' of standards; (iii) provide policy suggestions for designing an efficient ecosystem towards enabling an IoT environment. The total study cost is Rs. 19.20 lakhs for a duration of 06 months. The 1st instalment of Rs. 10.00 Lakhs was released to ICRIER, New Delhi *vide* sanction letter dated 25th April, 2019.

3. The key outcome/deliverables of the study which were stated by the ICRIER team are:

   a. The Study would be policy-oriented, where it will inform policy on the best approaches to governing standards which ensure conformity by Industry.
   b. It would be a novel study, aimed at exploring the realm of emerging technologies such as IoT, the implications of which are futuristic; it would sharpen from a policy perspective, the foresight and preparedness needed for embracing emerging technologies, especially for social well-being.
   c. The Study would contain an analysis of standard-setting processes and their institutional framework for existing technologies in India.
   d. The Study would provide a comprehensive analysis of emerging global practices on governance frameworks for standards in IoT and related infrastructure.
   e. The Study would provide policy recommendations on an institutional design that encourages the development of standards and their coordinated use by industry ,for technology diffusion.

4. During the PGRC meeting held via video conferencing on 22nd May 2020, the following work progress was reported by ICRIER, New Delhi.

   a. The Study started with an overview on growth of IoT, needs for standardization and the global landscape for standards-setting bodies in IoT.
   b. The Study identified the Standards Setting Bodies (SSO's) in India relevant to IoT linked initiatives; these were Telecommunication Standards Development Society

(TSDSI), Bureau of Indian Standards (BIS), Telecommunication Engineering Centres (TES), The seconded European Standardization Expert for India (SESEI), The Global ICT Standardisation Forum for India (GISFI), IOT for smart cities task force (IoT4SCTF) and India-EU cooperation on ICT-related standardization policy and legislation.

c. The Study highlighted the importance of SSOs, and where their composition & functioning plays a very important role in standardisation outcomes.
d. The Study has mentioned relationships between stakeholder identities, i.e., universities, individuals, Government, consumers, etc., with that of Standards and SSOs.
e. The Study has also looked into the aspect of mapping SSOs by knowledge areas of IoT, and highlighted the variety of ratification options followed by various IoT alliances.
f. The Study also presented case studies with respect to Industrial IoT, Consumer IoT and Smart cities in India.
g. A comparative study of the IoT policy of India with that of Singapore, Germany, UK, EU and USA was conducted.
h. The Study ended with varous policy recommendation such as setting clear & targeted policies for standards development, building research capabilities, strengthening governance of standards bodies and encouraging participation of states , MSMEs, start-ups etc.

Based on the project's progress and presentation made by the ICRIER, New Delhi during PGRC meeting, the following observations were made by the Committee:

a. The Committee felt that the study may present a brief overview of standards across the entire spectrum but must primarily focus on on IoT standards.
b. The Committee felt the need to highlight role of standards in IoT, not only in Smart Cities but also in specific application areas of IoT. It should also look at the impact of technologies such as Artificial intelligence, Virtual reality, Machine Learning etc.
c. It was suggested to include examples of how availability of IoT standards would assist the indigenous developers in providing cost-effective solutions, be it cobots,

digitization or AR/VR tools/software etc. to MSME & start-ups and reduce dependence on MNC players.

d. The Committee also suggested looking into the impact of SSOs in India and what they have achieved in terms of standards & standardisation. The Committee suggested listing out the achievements of BIS, TSDSI, &TEC and emphasised the need to collaborate.

e. It was suggested to list out the variety of open source standards, including current IoT standards being used in India. Based on the stakeholder feedback, the challenges faced in utilization of these standards, and further R&D required to refine the standards may also be covered in the study.

f. The Committee suggested to illustrate, with a detailed example, how India could participate & champion standards development at the global level.

6. The Committee agreed to close the study successfully if the suggestions made in the above paras are incorporated and a final report is accepted upon review by the Chairman & members. The PI was advised to revise and submit the final report before the end of June 2020.

7. The Meeting ended with the Chairman thanking all the members for their active participation and their valuable comments.

Sanjiva Prasad

Prof. Sanjiva Prasad
Chairman

Dr. Jitendra Kumar
Member

Sh. Ashwani Gupta
Co-Chairman

Dr Suman Mazumdar
Member Secretary

4

6.2 Approved Minutes of the Second PGRC Meeting

Government of India
Department of Scientific & Industrial Research
Ministry of Science and Technology,
Technology Bhawan, New Delhi - 16

Minutes of the Final Meeting of Project Guidance cum Review Committee (PGRC) for the study entitled "The **Role of Standards in Diffusion of Emerging Technologies: Internet of Things (IoT)**" by **the Indian Council for Research on International Economic Relations (ICRIER)**, New Delhi **under the A2K+ studies programme of DSIR.**

Date and Time: Wednesday, 18/09/2020, 3.00pm,
Venue: Via Vidyo Connect meeting platform
https://Desktopvc.nic.in/flex.html?roomdirect.html&key=Vk929PJJA4

The following PGRC members participated in the meeting to hold discussions on the status of study.

Sr. No	Name of the Member	Role
1	Prof. Sanjiva Prasad, Department of Computer Science and Engineering, IIT Delhi	Chairman
2	Dr. Vipin C. Shukla, Scientist-F, DSIR	Co-chairman
3	Shri Jitendra Kumar, Scientist D, Bureau of Indian Standards, New Delhi	Member
4	Dr. Kailash C. Petkar, Scientist-C, DSIR	Member Secretary

Other Participants who attended the meeting

1	Dr. Mansi Kedia, Fellow, ICRIER (Principal Investigator)
2	Ms. Richa Sekhani, Research Associate, ICRIER
3	Shri Naveen Chand, DSIR

PGRC member who could not attend the meeting

1	Smt. Kavita Bhatia, Scientist G, MeitY

Dr. Vipin C. Shukla, Scientist F, DSIR welcomed the Chairman and all the PGRC members and participants. He briefed about the previous meeting, role of PGRC in guiding the study towards meeting its objectives to complete the study and requested Chairman PGRC to conduct the meeting.

In his opening remarks, Chairman briefed about objective of the 2nd Meeting of PGRC and invited PI, Dr. Mansi Kedia, ICRIER to present the progress of the study so far highlighting recommendations made during the first PGRC meeting.

Summary of the discussions held and action points that emerged are given below –

1) Dr. Mansi Kedia presented the entire work including background, technical and financial progress of the study and details of work completed as per the recommendations of the first meeting of PGRC. Following are the key points that were highlighted and discussed during the meeting -

1

a. It was stated that the study was sanctioned on 25th April 2019 at the cost of Rs. 19.20 Lakhs for the duration of 6 months. DSIR has released Rs. 10.00 Lakhs as first instalment. The study was extended to up to June 2020 with the approval of Secretary, DSIR.
b. The broad objectives of the study were –
    i. To understand the role of standard setting organizations and the industry in setting and conforming standards.
    ii. To explore characteristics of an efficient architecture of standards.
    iii. To provide policy suggestions for designing an efficient ecosystem towards enabling an IoT environment.
c. PI discussed on standards developing organizations (SDOs) in IoT and all relevant standards in the IoT landscape with details on standard applicable to Industrial IoT, Consumer IoT and smart cities, both globally and India.
d. PI also highlighted the standards available for combination technologies such as Augmented Reality (AR), Virtual Reality (VR) and Mixed Reality (MR) and the potential of these technologies in India.
e. It was mentioned that the study has been updated with incorporation of open standards available and adopted in India for IoT.
f. PI further highlighted action taken on the recommendations of the first PGRC meeting and stated that relevant information with respect to all the recommendations have been incorporated in the report as per the following table-

Sr No.	Recommendation given during I PGRC meeting	Action taken by ICRIER
1.	The Committee felt that the study may present a brief overview of standards across the entire spectrum but must primarily focus on IoT standards.	The entire spectrum of IoT standards is reproduced in the report using an illustration borrowed from the *Alliance for Internet of Things (AIOTI) WG3 -Release 2.9.* In addition, PI compiled the IoT focused standards developed by various SDOs and alliances in **Appendix 1**. There is also a discussion on vertical specific standards across consumer IoT, industrial IoT, smart cities and combination technologies in Section 3 of the report.
2.	The Committee felt the need to highlight role of standards in IoT, not only in Smart Cities but also in specific application areas of IoT. It should also look at the impact of technologies such as Artificial intelligence, Virtual reality, Machine Learning etc.	The potential for AR, VR and MR as combination technologies along with IoT and AI have been incorporated in **Section 3.1** using examples of applications in Industrial IoT. **Table 3.1 in Section 3.1.1** summarizes the standards that are under consideration for AR, VR and MR.
3.	It was suggested to include examples of how availability of IoT standards would assist the indigenous developers in providing cost-effective solutions, be it cobots, digitization or AR/VR to	Integration of MSMEs and their role in standard development and standard adoption has been elaborated in **Section 5.4 of the report.**

	MSME and startups and reduce dependence on MNC players.	
4	Impact of SSO in India and what they have achieved in terms of standards and standardization. The committee suggested listing out the achievements of BIS, TSDSI and TEC and need to collaborate	The achievements of Indian SDOs is incorporated in **Section 2.3** and the list of standards are provided in **Appendix 2** and **Section 3.3.1** for development of Smart Cities. The need to collaborate and methods of collaboration run through several points in the recommendations.
5	List out variety of Open standards, including current IoT standards being used in India. Based on the stakeholder feedback, the challenges faced in utilisation of standards and further R &D required to refine the standards may also be covered	The discussion on a specific open source standard attracting traction in India is explained in **Section 3.2** in the context of Consumer IoT. Other open source initiatives are explained in **Section 2.2** and **Appendix 3** on the IoT OSS Initiative
6	List out an example of how India can participate and champion standards development at global level	This has been elaborated in the recommendations **Section 5**

a. PI further presented recommendations on the integration of MSMEs to the standards ecosystem including the need for process alignment and computerization of the shop floor.
b. PI also highlighted the recommendations regarding the need for stakeholders to collaborate and work collectivity, the need for integrating startups and MSMEs in the standards ecosystem, the need for cyber security standards, the need for certification agencies for new standards based products, the need for harmonization of smart cities standards, etc.
c. After discussing the achievements of objectives, PI informed PGRC that SE/UC is already submitted and requested for the release of second and third installment.
d. Finally, PGRC appreciated the efforts of PI in conducting this exhaustive study. Based on the detailed deliberation on the presentation of PI, PGRC placed following recommendations for PI.

Recommendations of the PGRC:

1. PGRC was satisfied with the actions taken by ICRIER on all the recommendations made during first PGRC meeting. In view of this, the committee accepted the report submitted by ICRIER. However, formatting of the report may be done in consultation with DSIR.
2. PGRC recommended release of second installment of Rs. 7.00 lakhs to ICRIER.
3. PGRC also recommended to release third/balance installment to ICRIER after approval of the completion of report by DSIR.

The meeting concluded with thanks to all the participants for their valuable contribution.

3

As approved by Chairman, PGR

7. References

Ackerman. L (2013). "Mobile Health and Fitness Applications and Information Privacy Report to California Consumer Protection Foundation", July 15. 2013.

Allen. R and Sriram R (2000). "The Role of Standards in Innovation", *Technological forecasting and social change*, 64, 171-181 (2000), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=821473

Antipolis. S (2019). oneM2M announced as the "Top IoT Standards Body of the Year", ETSI. https://www.etsi.org/newsroom/news/1582-2019-04-onem2m-announced-as-the-top-iot-standards-body-of-the-year

Ashton. K (2009) "That 'Internet of Things' Thing". *RFID Journal,* June 22, 2019. https://www.rfidjournal.com/articles/pdf?4986

Ashwin (2015). "Evolution of Keyboards: Why Is Qwerty the Most Preferred Keyboard?", *Science ABC*, June 24, 2015. https://www.scienceabc.com/innovation/qwerty-keyboard-over-the-years-why-is-it-the-most-preferred-typing-tool.html

Balaji. S (2019). "OCF India Chapter: India's IoT market is ready for standardization norms", Na*sscom Community*, May 21, 2019. https://community.nasscom.in/communities/iot-ai/ocf-india-chapter-indias-iot-market-is-ready-for-standardization-norms.html

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

Basulto. D (2015). "3 reasons why the Internet of Things (still) doesn't make sense". *The Washington Post.*

Carrier. M (2009), "Innovation for the 21st Century: Harnessing the Power of Intellectual Property and Antitrust Law", *Oxford University Press.*

Cisomag (2020). "All You Need to Know About India's First Data Protection Bill", *Cisomag*, January 3, 2020. https://www.cisomag.com/all-you-need-to-know-about-indias-first-data-protection-bill/

Chowdhary. S (2019). "Home automations: Making our homes smart and connected", *Financial Express*, June 6, 2019. https://www.financialexpress.com/industry/technology/home-automations-making-our-homes-smart-and-connected/1599137/

Darmois. S, Daniele. L, Guillemin. P, Heiles. J, Moretto. P and Van der Wees. A (2017) "IoT Standards Landscape – State of the Art Analysis and Evolution". https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609105C6.pdf

Dedhia. Z (2014). "The Secret History of Keyboards (QWERTY vs DVORAK)", *TechTricks World,* August 24, 2014. https://www.techtricksworld.com/secret-history-keyboards-qwerty-vs-dvorak/

Evans. D (2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*". Cisco Internet Business Solutions Group (IBSG),* April 2011.

Gerundino. D, Weissinger. R, Grosfort. J and Diamond. X (2014). "Economic Benefits of Standards". International Standards Organisation (ISO), https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/ebs_case_studies_factsheets.pdf

Hoppe. S (2017). "There Is No Industry 4.0 without OPC UA". *Automation.com* https://www.automation.com/automation-news/article/there-is-no-industry-40-without-opc-ua

Kapoor. V and Nagpal. P, "Intellectual Property Rights and Small Medium Enterprises (SME's)", International Journal of Law and Legal Jurisprudence Studies, ISSN-2348-8212 http://ijlljs.in/intellectual-property-rights-and-small-medium-enterprises-smes/

Kiss. J (2010). "Google admits collecting Wi-Fi data through Street View cars", *The Guardian*, 15 May 2010.

Katz. M and C. Shapiro (1985). "Network Externalities, Competition and Compatibility." *American Economic Review* "75 (3):424-40

Kunt. B (2013). "The Impact of Standardization and Standards on Innovation". *Manchester Institute of Innovation Research*, Nesta Working Paper No. 13/15

Manos. A, et al (2017). "Understanding the mirai botnet." *26th {USENIX} Security Symposium ({USENIX} Security 17).* 2017

Manyika. J, Woetzel. J, Dobbs. R, Bison. P, Bughin. J and Aharon. D (2015). Unlocking the potential of the Internet of Things, *McKinsey Global Institute*, June 2015

Meddeb. A (2016). "Internet of things standards: who stands out from the crowd?". IEEE Communication Magazine, Volume 54, Issue 7, July 2016. Page 40-47

Muppiri. C (2019). "Public-Private Partnerships in Indian Industrial IoT a Set of Policy Recommendations to Improve Cyber Security", *Cybersecurity Academy*. https://d1rkab7tlqy5f1.cloudfront.net/TBM/Over%20faculteit/Afdelingen/Engineering%20Systems%20and%20Services/People/Professors%20emeriti/Jan%20van%20den%20Berg/MasterPhdThesis/PPP%20in%20Indian%20IIoT_Chandra_Thesis%20%20Final.pdf

Noura. M (2018). Interoperability in Internet of Things: Taxonomies and Open Challenges, *Mobile Networks and Applications*, 2019, Volume 24, Number 3, Page 796

Pal. A, Rath. H, Shailendra. S and Bhattacharyya. A (2018). "IoT Standardization: The Road Ahead" Submitted: September 30th 2017Reviewed: February 9th 2018Published: March 29th 2018 DOI: 10.5772/intechopen.75137

Priya (2019). "Future of IoT in India – Current Market Trends and Use Cases", Wire 19. https://wire19.com/future-of-iot-in-india-current-market-trends-and-use-cases/

Rawlinson. K (2014) "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", HP, July 29, 2014. https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

Robertson. A (2019). "Competitors say Qualcomm is running a monopoly — here's why", *The Verge*, January 9, 2019. https://www.theverge.com/2019/1/9/18173756/qualcomm-ftc-antitrust-monopoly-trial-explainer

Rose. K, Eldridge. S and Chapin. L (2015). "THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World", Internet Society.

Saleem. J, Hammoudeh. M, Raza. U, Adebisi. B, and Ande. R (2018). "IoT Standardisation - Challenges, Perspectives and Solution". In Proceedings of ICFNDS' 18, Amman, Jordan, June 26-27, 2018, 9 pages. DOI:hŠps://doi.org/10.1145/3231053. 3231103

Schneier.B (2015). "How the Internet of Things Limits Consumer Choice", *The Atlantic*. December 24, 2015. https://www.theatlantic.com/technology/archive/2015/12 /internet-of-things-philips-hue-lightbulbs/421884/

Sivakumaran. M and Castells. P (2019). "The contribution of IoT to economic growth Modelling the impact on business productivity". *GSMA Intelligence*, April 2019.

Tandon, P. (2016). "Internet of Things: The next evolutionary step- A Review". *International Journal of Students' Research in Technology & Management*, *4*(2), 30-34. Retrieved from http://giapjournals.com/index.php/ijsrtm/article/view/ijsrtm .2016.422

Tan. A (2018). "Singapore government outlines its approach to IoT". *computerWeekly.com,* March 21, 2018. https://www.computerweekly.com/news/252437239/Singapore-government-outlines-its-approach-to-IoT

Undegrove. A. "Participating in Standard Setting Organizations: Value Propositions, Roles and Strategies*", ConsortiumInfo.org. https://www.consortiuminfo.org/essentialguide/participating1.php*

Wigmore I. (2014). "Internet of Things (IoT)". *TechTarget,* 28 July 2019.

Woo, J. J. (2017). "Singapore's Smart Nation Initiative–A Policy and Organisational Perspective". *Lee Kuan Yew School of Public Policy, National University of Singapore*.

8. Appendix

Appendix 1: Scope and objectives of the various SDOs and alliances involved in developing standards for IoT

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
International Telecommunication Union (ITU)	1865	ITU's global membership includes 193 Member States as well as some 900 companies, universities, and international and regional organizations.	Telecommunication	It's Global Standards Initiative (IoT-GSI) intends to act as an umbrella for all IoT standardisation activities so that IoT can be enabled on a global scale. It defines all layers and protocols for connectivity and ensures interoperability with all standards from diverse SDOs. It's security and privacy guidelines conform with solutions from other SDOs/	Core / Communication / Messaging
				· **SG** (Study Group) **13**: Recommendations defining IoT and outlining functional requirements of machine-oriented communication applications in an NGN (Next generation network) context.	
				· **SG 15**: Working on communication aspects of Smart grids. **G.9903** and **G.9905** are some recommendations.	
				· **SG 17**: Cybersecurity and Identity Management for IoT and related technologies like smart grids, cloud computing and web services.	
				· **SG 20**: "IoT and its applications, including smart cities and communities"	

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
ISO/IEC (International Organization of Standardisation and International Electro technical Commission)	ISO: 1947 IEC: 1906	ISO: Members from 164 countries and 780 technical committees and subcommittees to take care of standards development IEC: Standards for all electrical, electronic and related technologies. These are known collectively as "electrotechnology".	ISO: published over 22803 International Standards covering almost all aspects of technology and manufacturing IEC: Close to 20 000 experts from industry, commerce, government, test and research labs, academia and consumer groups participate in IEC Standardisation work.	ISO/IEC JTC 1/SWG 5 Internet of Things (IoT) is a standardisation special working group (SWG) of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardisation (ISO) and the International Electro Technical Commission (IEC), which develops and facilitates the development of standards for Internet of Things (IoT). ISO/IEC JTC 1/SWG 5 was established in 2012 at the 27th plenary meeting of ISO/IEC JTC 1 in Juju **ISO/IEC 30141,** Internet of Things (IoT) – Reference architecture, provides an internationally standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practice. **ISO/IEC 21823-1**:2019(E) provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems	Core / Communication / Messaging
IETF (Internet Engineering Taskforce) and Internet Research Task Force (IRTF)	1986		Automated Network management, The Internet of Things, New Transport Technology, Security and Privacy	DTLS - Datagram Transport Layer Security UDP - User Datagram Protocol IPv6 - Internet Protocol, Version 6 Core is providing a framework for resource-oriented applications intended to run on constrained IP networks. ROLL - Routing Over Low power and Lossy	Core / Communication / Messaging

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
				networks Cap - Constrained Application Protocol 6LoWPAN - IPv6 over Low power Wireless Personal Area Networks XMPP - Extensible Messaging and Presence Protocol - XMPP IoT HTTP - Hypertext Transfer Protocol	
The Institute of Electrical and Electronics Engineer (IEEE)	1963	more than 423,000 members in over 160 countries,	electrical and electronics	More than 80 standards are available and 45 standards relating to IoT is being developed. Some of them are: IEEE 802.3 Ethernet IEEE 1901 - Broadband over Power Line Networks IEEE 802.15.4e - IEEE Standard for Local and metropolitan area networks IEEE 802.15.4g - Physical Layer (PHY) IEEE 802.11 - WIFI	Core / Communication / Messaging
Regional Standard Bodies					

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
The European Telecommunications Standards Institute (ETSI)	1988	ETSI counts more than 850 member organizations worldwide, drawn from 65 countries and five continents.	4G and 5G mobile communications and machine to machine communication. "Produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, aeronautical, broadcast and internet technologies" - Within ETSI various applications of M2M technology: Smart appliances Smart metering Smart cities – Smart grids, eHealth Telemedicine are addressed	IoT Focused Protocols including Low Throughput Networks (LTN). Approximately 90 standards on IoT is developed	Long Range
Alliance/ Consortia					
OneM2M	2012	It is backed by 8 leading standardisation organsiation and 6 industry consortia with more than 200 participating members.	Technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective	A set of 10 specifications, covering requirements, architecture, API specifications, security solutions and mapping to common industry protocols such as CoAP, MQTT and HTTP. oneM2M Release 1 also makes use of OMA and Broadband Forum specifications for Device Management capabilities. Existing Standards like LoRA (Long Range Radio), NB-IoT, CoAP (Constrained Application	Multi-Layer/ Stack Initiatives

IoT Alliances/ Consortia / Standard Bodies	Year of Establish ment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
			of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc.	Protocol), HTTP and MQTT are used in the oneM2M framework.	
The 3rd Generation Partnership Project (3GPP)	1998		GSM and related 2G / 2.5G standards including GPRS and EDGE. UMTS and related 3G standards including HSPA LTE and related 4G standards An evolved IP Multimedia Subsystem (IMS) developed in an access independent manner 5G standards	Developed a radio standard called Narrowband IoT (NB-IoT) in June 2016 which was developed for LPWAN (Low Powered Wide Area Network) to support IoT technologies. However, backwards compatibility and privacy still needs to be addressed	
				Low energy consumption is one of the central agendas for IoT standards development	
				Has identified ways to increase the coverage of LTE. LTE Release 12 introduces a power save mode and simplified signaling procedures to provide additional battery savings.	
				Also working on technologies like Extended Coverage GSM Internet of Things (EC-GSM-IoT) and LTE for Machine type communications (LTE-M).	

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
Open Connectivity Foundation (OCF)	2016	over 300-member organisation	Automotive, Healthcare, Smart Building, Smart Home, Security, Collateral	One of the active SDOs in the IoT ecosphere, OCF commenced the IoTivity project, an open source software framework for enabling device to device connectivity and interoperability.	Multilayer / Stack Initiatives
Organisation for the Advancement of Structured Information Standards (OASIS)	1993	more than 2,000 participants representing over 600 organizations and individual members in more than 65 countries.	security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas	AMQP: Advanced Message Queuing Protocol - Royalty free license "An open standard for passing business messages between applications or organizations. It connects systems, feeds business processes with the information they need and reliably transmits onward the instructions that achieve their goals." MQTT: Message Queuing Telemetry Transport - Royalty free license "It was designed as an extremely lightweight publish/subscribe messaging transport." oBIX: Open Building Information Exchange	Long Range
World Wide Web Consortium (W3C)	1994		Web standards	An international community that develops open standards to ensure the long-term growth of the Web. It aims to achieve the mentioned objectives through standard complementing building blocks (like metadata and APIs) that enable easy access across IoT platforms and application domains.	Core / Communication / Messaging

IoT Alliances/ Consortia / Standard Bodies	Year of Establish ment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
Lora Alliance	2015	more than 500 members	Internet of Things (IoT), machine-to-machine (M2M), and smart city, and industrial applications	LoRaWAN network protocol Tech Overview Data Rates: Range from 0.3 kbps to 50 kbps. Distance: 100 km (62 miles) in favorable environments Battery: Sensors can run for 10 years or more on a single AA battery Security: Unique Network key (EUI64) and ensure security on network level Unique Application key (EUI64) ensure end to end security on application level Device specific key (EUI128) IBM LoRa WAN in C - Eclipse Public License - Developer Portal	Long Range
Open Mobile Alliance (OMA)	2018	101	The OMA SpecWorks working groups are active in a variety of technologies including messaging, location, device management, APIs, IoT and machine-to-machine device communication.	OMNA Lightweight M2M (LWM2M) "OMA Lightweight M2M standard for Device Management, Network Management and Application Data for the Internet of Things. This new CoAP and DTLS based standard provides a complete system interface solution for M2M devices and services."	Long Range
Hypercat	2014	60+		"HyperCat makes services machine-browsable" JSON-based hypermedia catalogue format for exposing collections of URIs. Each HyperCat catalogue may expose any	Semantics

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
				number of URIs, each with any number of RDF-like triple statements about it.	
Continua	2006	200+	Health Alliance: medical-grade health/sensor data to flow from a multitude of vital signs devices used by consumers to health services, all the way into local, regional or national EHRs and data lakes in a safe and secure manner.	"Developing design guidelines that will enable vendors to build interoperable sensors, home networks, telehealth platforms, and health and wellness services. Establishing a product certification program with a consumer-recognizable logo signifying the promise of interoperability across certified products. Collaborating with government regulatory agencies to provide methods for safe and effective management of diverse vendor solutions. Working with leaders in the health care industries to develop new ways to address the costs of providing personal telehealth systems."	Vertical / Industry Focused
Thread Group			**Thread** is a low power, secure and Internet-based mesh networking technology for home and commercial IoT products.	Thread is a low-power wireless mesh networking protocol, based on the universally-supported Internet Protocol (IP), and built using open and proven standards. Thread enables device-to-device and device-to-cloud communications and reliably connects hundreds (or thousands) of products and includes mandatory security features. Thread networks have no single point of	Vertical / Industry Focused

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
				failure, can self-heal and reconfigure when a device is added or removed, and are simple to setup and use. Thread is based on the broadly supported IEEE 802.15.4 radio standard, which is designed from the ground up for extremely low power consumption and low latency.	
The Industrial Internet Consortium (IIC)	2014	More than 250 members	Energy, Transportation, Healthcare and Smart Cities sectors.	The IIC does not adopt technical specifications or specify technologies to be used, but may from time to time recommend that particular standard-setting or specification-development projects be undertaken under the management and rules of Object Management Group (OMG) or other standards setting organizations. “Editor’s Note: OMG specs related to IoT include: Data Distribution Service (DDS) Unified Component Model for Distributed, Real-Time and Embedded Systems More Details The IIC has established the following liaisons: The Eclipse Foundation GS1 OASIS Object Management Group The Open Group	Industrial IoT

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
				Open Interconnect Consortium Smart Grid Interoperability Panel (SGIP) etc.	
The Internet of Things Consortium		56 members	Driving adoption of IoT products & services through consumer research and market education."	IoT Network: Companies, executives and resources in the IoT consumer product space IoTC Committees: Representatives from each member company that help deliver the IoTC vision Market Development: Participate in defining new markets and making them accessible to IoT companies (consumer, retail, foreign) Events: IoT events focused on product development and consumer adoption trends Demos: Ability to participate in consumer focused IoT demos (i.e. SmartThings connected house) Awareness: Product awareness and promotion via IoTC (website, press, events)	Industry Marketing / Education Focused
YRP Ubiquitous Networking Laboratory	2002		Aim of achieving a ubiquitous computing environment that supports our lives in a sophisticated manner by embedding microcomputers with communication capabilities, sensors, actuators, etc. in all physical objects around us and having them operate in a concerted manner by exchanging information with	Develops the application framework that integrates various technologies for location identification. Development is focused on the basic technologies of the IoT such as integrated location management system by uID architecture and the technology to deliver information according to context such as the interest and current location of users	OpenData/ Smart City Solutions

IoT Alliances/ Consortia / Standard Bodies	Year of Establishment	Total Members	Focus Area	IoT Focused efforts / Standards	Category
			each other. Establishing next-generation protocols for the communication as the infrastructure of ubiquitous computing is another major goal of YRP UNL.		
GS1/ EPC Global	1974		To innovate and develop industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID) and allow global visibility of items (EPCIS) in today's fast-moving, information rich, trading networks	Standards have been developed in two areas: 1. EPC/RFID tags 2. EPC Information services	Network focused
Open Geospatial Consortium		More than 350 members	Defines and maintains standards for location-based, spatial-temporal data and services. Strives towards developing quality open standards for the geo-spatial community	**Some of the work is related to IoT**, e.g. a modular suite of standards for web services allowing ingestion, extraction, fusion, and (with the web coverage processing service (WCPS) component standard) analytics of massive spatio-temporal data like satellite and climate archives	Geospatial/Mapping/Communication

Source: Compiled by authors from website of SDOs and alliances

Appendix 2: Achievements of BIS and TSDSI

Bureau of Indian Standards

IoT related standards can be found under different working groups of the Electronics and Information Technology Department (LITD) of BIS. The table below provides a snapshot of such published standards under the new BIS interface.

Working Group	Sr. No	Standard	Standard Title	Category
LITD 27: Internet of Things and Related Technologies		IS/ISO/IEC/TR 22417 : 2017/ISO/IEC TR 22417:201	Information Technology: "Internet of Things" IoT Use Cases	Code of Practice
LITD 32: Biometrics		IS 16464 : Part 1 : 2019/ISO/IEC 19784-1:2018	Information Technology - Biometric Application Programming Interface Part 1 BioAPI Specification	Others
		IS 16464 : Part 2 : 2016	Information technology - Biometric application programming interface: Part 2 biometric archive function provider interface	Others
		IS 16464 : Part 4 : 2015	Information technology - Biometric application programming interface: Part 4 biometric sensor function provider interface	Others
		IS 29109 : Part 2 : 2010/ISO/IEC 29109-2:2010	Information Technology - Conformance Testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 2 Finger Minutiae Data	Others
		IS/ISO/IEC 19794 : Part 1 : 2011/ISO/IEC 19794-1 : 2011	Information Technology - biometric Data interchange formats part 1 Framework	
		IS/ISO/IEC 19794 : Part 10 : 2007/ISO/IEC 19794-10:200	Information Technology - Biometric Data Interchange Formats Part 10 hand Geometry Silhouette Data	Methods of tests
		IS/ISO/IEC 19794 : Part 11 : 2013/ISO/iEC 19794-11 : 2013	Information Technology - Biometric Data Interchange Formats Part 11 Signature/Sign Processed Dynamic Data	Others
		IS/ISO/IEC 19794 : Part 13 : 2018/ISO/IEC 19794-13:201	Information Technology - Biometric Data Interchange Formats Part 13 Voice Data	Others

Working Group	Sr. No	Standard	Standard Title	Category
		IS/ISO/IEC 19794 : Part 14 : 2013/ISO/IEC 19794-14:2013	Information technology - Biometric data interchange formats: Part 14 dna data	Others
		IS/ISO/IEC 19794 : Part 15 : 2017/ISO/IEC 19794-15:201	Information Technology - Biometric Data Interchange Format Part 15 Palm Crease Image Data	Others
		IS/ISO/IEC 19794 : Part 2 : 2011/ISO/IEC 19794-2:2011	Information Technology - Biometric Data Interchange Formats Part 2 Finger Minutiae Data	Others
		IS/ISO/IEC 19794 : Part 3 : 2006/ISO/IEC 19794-3:2006	Information Technology - Biometric Data Interchange Formats Part 3 Finger Pattern Spectral Data	Others
		IS/ISO/IEC 19794 : Part 4 : 2011/ISO/IEC19794-4 : 2011	Information Technology - Biometric Data Interchange Formats Part 4 Finger Image Data	Others
		IS/ISO/IEC 19794 : Part 5 : 2011/ISO/IEC 19794-5:2011	Information Technology - Biometric Data Interchange Formats Part 5 Face Image Data	Others
		IS/ISO/IEC 19794 : Part 6 : 2011/ISO/IEC 19794-6:2011	Information Technology - Biometric Data Interchange Formats Part 6 Iris Image Data	Others
		IS/ISO/IEC 19794 : Part 7 : 2014/ISO/IEC 19794-7 : 2014	Information Technology - biometric Data interchange formats part 7 Signature/Sign Time Series Data	Others
		IS/ISO/IEC 19794 : Part 8 : 2011/ISO/IEC 19794-8:2011	Information technology - Biometric data interchange formats: Part 8 finger pattern skeletal data	Others
		IS/ISO/IEC 19794 : Part 9 : 2011/ISO/IEC 19794-9 : 2011	Information Technology - biometric Data interchange formats part 9 vascular image Data	
		IS/ISO/IEC 29109 : Part 1 : 2009/ISO/IEC 29109-1 : 2009	Information Technology - Conformance testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 1 Generalized Conformance Testing Methodology	Methods of tests
		IS/ISO/IEC 29109 : Part 10 : 2010/ISO/IEC 29109-10 : 2010	Information Technology - Conformance Testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 10 Hand Geometry Silhouette Data	
		IS/ISO/IEC 29109 : Part 4 : 2010/ISO/IEC 29109-4:2010	Information technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794: Part 4 finger image data	Others

Working Group	Sr. No	Standard	Standard Title	Category
		IS/ISO/IEC 29109 : Part 5 : 2014/ISO/IEC 29109 : Part 5 : 2014	Information technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794: Part 5 face image data	Others
		IS/ISO/IEC 29109 : Part 6 : 2011/ISO/IEC 29109-6 : 2011	Information Technology - Conformance Testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 6 Iris Image Data	
		IS/ISO/IEC 29109 : Part 7 : 2011/ISO/IEC 29109-7 : 2011	Information Technology - Conformance Testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 7 Signature/Sign Time Series Data	Others
		IS/ISO/IEC 29109 : Part 8 : 2011/ISO/IEC 29109-8 : 2011	Information technology - Conformance Testing Methodology For Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 8 Finger Pattern Skeletal Data	Others
		IS/ISO/IEC 29109 : Part 9 : 2011/ISO/IEC 29109-9 : 2011	Information Technology - Conformance Testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794 Part 9 vascular image Data	Others
		IS/ISO/IEC/TR 29196 : 2018/ISO/IEC TR 29196:201	Information Technology - Guidance for Biometric Enrolment	Others

However, in the previous BIS website interface, one could view certain standards undergoing deliberations. They have been listed below.

Working Group	Sr. No.	Standard	Standard Title	Status
LITD 27: IoT and Related Technologies	1.	LITD/27/13076	INFORMATION TECHNOLOGY UNDERWATER ACOUSTIC SENSOR NETWORK UWASN PART 1: OVERVIEW AND REQUIREMENTS	WC-Draft
LITD 28: Smart Infrastructure	1.	LITD/28/13485	Information technology Unified ICT architecture for Smart Infrastructure - Last Mile Communication Protocol Stack Architecture - Sub Giga Hz PHY	Project-Approval

	2.	LITD/28/13499	Information technology Unified ICT architecture for Smart Infrastructure - Last Mile Communication Protocol Stack Architecture - Overview	Project-Approval
	3.	LITD/28/13502	Information Technology - Unified Digital Infrastructure - Unified Last Mile Communication Protocols Stack - Reference Architecture (UDI – ULMCPS - RA)	WC-Draft
	4.	LITD/28/13503	Information Technology - Unified Digital Infrastructure - Unified Last Mile Communication Protocols Stack - Network Access Layer (Sub Giga Hz)	WC-Draft
	5.	LITD/28/14048	IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control MAC and Physical Layer PHY Specifications	Accepted
	6.	LITD/28/14051	IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control	Accepted
	7.	LITD/28/14054	IEEE Standard for Low-Rate Wireless Networks	Accepted
	8.	LITD/28/14060	IEEE Recommended Practice for Transport of Key Management Protocol KMP Datagrams	Accepted
	9.	LITD/28/14073	Smart Infrastructure - Data Exchange Framework: Part 1 Reference Architecture	P-Draft
	10.	LITD/28/14079	Unified Resilient Secure Sustainable Smart Infrastructure ICT Reference Architecture	P-Draft
	11.	LITD/28/14080	Unified ICT architecture for Smart Infrastructure Common Service Layer	Project-Approval
LITD 30: Artificial Intelligence	1.	LITD/30/15000	Information technology Big data Overview and vocabulary	WC Draft

Source: Compiled by authors

Telecommunications Development Society, India (TSDSI)

TSDSI has one published standard called CPRI Fronthaul Standard which specifies the functional block for fronthaul processing for transport of Common Public Radio Interface (CPRI) and/or GE from the Base Band Unit (BBU) or Radio Equipment Control (REC) to the Remote RadioHead (RRH) or Radio Equipment (RE) of a base station. Its other standards are transposed from 3GPP and ITU and OneM2M. These have been summarised below.

OneM2M Spec. Title	oneM2M TS	oneM2M Version	TSDSI Standard Number
Functional Architecture	TS-0001	v2.10.0	TSDSI STD T1.oneM2M TS-0001-2.10.0 V1.0.0
Requirements	TS-0002	v2.7.1	TSDSI STD T1.oneM2M TS-0002-2.7.1 V1.0.0
Security Solutions	TS-0003	v2.4.1	TSDSI STD T1.oneM2M TS-0003-2.4.1 V1.0.0
Service Layer Core Protocol	TS-0004	v2.7.1	TSDSI STD T1.oneM2M TS-0004-2.7.1 V1.0.0
Management Enablement (OMA)	TS-0005	v2.0.0	TSDSI STD T1.oneM2M TS-0005-2.0.0 V1.0.0
Management enablement (BBF)	TS-0006	v2.0.1	TSDSI STD T1.oneM2M TS-0006-2.0.1 V1.0.0
Service Components	TS-0007	v2.0.0	TSDSI STD T1.oneM2M TS-0007-2.0.0 V1.0.0
HTTP Protocol Binding	TS-0009	v2.6.1	TSDSI STD T1.oneM2M TS-0009-2.6.1 V1.0.0
MQTT protocol binding	TS-0010	v2.4.1	TSDSI STD T1.oneM2M TS-0010-2.4.1 V1.0.0
Common Terminology	TS-0011	v2.4.1	TSDSI STD T1.oneM2M TS-0011-2.4.1 V1.0.0
Base Ontology	TS-0012	v2.0.0	TSDSI STD T1.oneM2M TS-0012-2.0.0 V1.0.0
LWM2M Interworking	TS-0014	v2.0.0	TSDSI STD T1.oneM2M TS-0014-2.0.0 V1.0.0
Testing Framework	TS-0015	v2.0.0	TSDSI STD T1.oneM2M TS-0015-2.0.0 V1.0.0
WebSocket Protocol Binding	TS-0020	v2.0.0	TSDSI STD T1.oneM2M TS-0020-2.0.0 V1.0.0
oneM2M_and_AllJoyn_Interworking	TS-0021	v2.0.0	TSDSI STD T1.oneM2M TS-0021-2.0.0 V1.0.0
Home Appliances Information Model and Mapping	TS-0023	v2.0.0	TSDSI STD T1.oneM2M TS-0023-2.0.0 V1.0.0
OICInterworking	TS-0024	v2.0.0	TSDSI STD T1.oneM2M TS-0024-2.0.0 V1.0.0
Use Cases Collection	TR-0001	v2.4.1	TSDSI STD T1.oneM2M TR-0001-2.4.1 V1.0.0
Study on Abstraction and Semantics Enablement	TR-0007	v2.11.1	TSDSI STD T1.oneM2M TR-0007-2.11.1 V1.0.0
Security	TR-0008	v2.0.0	TSDSI STD T1.oneM2M TR-0008-2.0.0 V1.0.0
End-to-End-Security and Group Authentication	TR-0012	v2.0.0	TSDSI STD T1.oneM2M TR-0012-2.0.0 V1.0.0
Authorization Architecture and Access Control Policy	TR-0016	v2.0.0	TSDSI STD T1.oneM2M TR-0016-2.0.0 V1.0.0
Home Domain Abstract Information Model	TR-0017	v2.0.0	TSDSI STD T1.oneM2M TR-0017-2.0.0 V1.0.0
Industrial Domain Enablement	TR-0018	v2.0.0	TSDSI STD T1.oneM2M TR-0018-2.0.0 V1.0.0
Dynamic Authorization for IoT	TR-0019	v2.0.0	TSDSI STD T1.oneM2M TR-0019-2.0.0 V1.0.0
Continuation and Integration of HGI Smart Home activities	TR-0022	v2.0.0	TSDSI STD T1.oneM2M TR-0022-2.0.0 V1.0.0
3GPP_Rel13_IWK	TR-0024	v2.0.0	TSDSI STD T1.oneM2M TR-0024-2.0.0 V1.0.0

Appendix 3: Comparing IoT OSS Initiative

IoT OSS Initiatives	Scope	Domain	Application Areas	IPR Policy
Civil Infrastructure Platform (CIP)	Infrastructure knowledge area (SW Platform, Operating System).	Industrial, Service & App (SW platform).	Any technical systems responsible for supervision, control, and management of infrastructure supporting human activities, including, for example, electric power generation and energy distribution, oil and gas, water and wastewater, healthcare, communications, transportation, and community management	
Eclipse IoT-Testware	· Communication and Connectivity knowledge area. · Integration/Interoperability knowledge area. · Applications knowledge area. · Infrastructure knowledge area. · IoT Architecture knowledge area. · Devices and sensor technology knowledge area. · Security and Privacy knowledge area.	Initiative is related to multiple market domains (consumer/industrial internet) and the technical domain (connectivity, service e& applications),		Eclipse Public License 1.0
IoTivity	· Communication and Connectivity knowledge area. · Integration/Interoperability knowledge area. · Applications knowledge area. · Infrastructure knowledge area.	Multiple domains – initial release has a consumer focus with a mix of connectivity and services.	Different specifications cover different areas. The initial focus is on Smart Home.	FRAND – Free licensing.

IoT OSS Initiatives	Scope	Domain	Application Areas	IPR Policy
	· IoT Architecture knowledge area. · Devices and sensor technology knowledge area. · Security and Privacy knowledge area.			
IoT6		IoT6 encompasses both consumer and industrial Internet. • It encompasses both connectivity and application layers, with a cross domain positioning.	IoT6 is fully cross-domain, encompassing smart buildings, smart cities, smart agriculture, etc.	Part of the specifications are open, specific access rules are defined by IoT6.
OM2M (Open platform for M2M)	•Integration/Interoperability knowledge area: • IoT Architecture knowledge area: • Security and Privacy knowledge area:	OM2M creates horizontal service and allows to create applications. It concerns B2C and B2B.	OM2M creates a complete IoT solutions for horizontal industry. Several companies and research laboratories use OM2M in different domains: smart-building, transportation, healthcare, energy and smart cities.	Eclipse Public License (EPL).
sensiNact (aka BUTLER platform)	· Communication and Connectivity knowledge area. · Integration/Interoperability knowledge area. · Applications knowledge area. · Infrastructure knowledge area. · IoT Architecture knowledge area. · Devices and sensor technology knowledge area. · Security and Privacy knowledge area.	sensiNact is a platform for managing IoT services & applications. It is domain agnostic and can be applied to consumer or industrial business.	sensiNact is focusing the horizontal industry, a plug & play application platform for various IoT vertical domains. Deployments in smart home, smart office, smart transportation, and smart city have already been done	Apache Software License 2.0.

IoT OSS Initiatives	Scope	Domain	Application Areas	IPR Policy
Sofia2	· Communication and Connectivity knowledge area. · Integration/Interoperability knowledge area. · Applications knowledge area. · Infrastructure knowledge area. · IoT Architecture knowledge area. · Devices and sensor technology knowledge area. · Security and Privacy knowledge area.	Horizontal IoT Platform with Big Data and Analytics Capabilities for developing Vertical Solutions. Domain agnostic, applicable to enterprise business mainly. • On the quadrant Sofia2 (horizontal axis on Industrial Internet Market although Sofia2 is also used on Consumer Market, vertical Axis as Core for Service & Apps).	As Horizontal IoT Platform can be used in any industry: Smart Cities, Energy, Health, Home, Transportation, Finance, Security, Insurance, Banking, Manufacturing, Industry, Office. • Sofia2 has already deployments on Smart Cities, Smart Energy, Smart Home, Smart Health, Smart Transportation, Smart Banking. • Sofia2 is focusing on the creation of complete IoT Solutions working as the core of these solutions.	Open Source Version: Platform on AGPL v3 (GNU Affero General Public License). APIS on Apache 2.0. • Commercial Version: different models.
UniversAAL IoT	· Communication and Connectivity knowledge area. · Integration/Interoperability knowledge area. · Applications knowledge area. · Infrastructure knowledge area. · IoT Architecture knowledge area. · Devices and sensor technology knowledge area. · Security and Privacy knowledge area.	universAAL sits on top of different connectivity solutions and provides for semantic communication and compatibility; this framework can be used for integrating arbitrary service and application components, even platform-level service components. universAAL's own "manager" components (platform-level service components) are the same way pluggable and substitutable like the application-level components. universAAL can be used for integrating arbitrary open distributed systems of systems (and	universAAL provides a horizontal service and application integration layer across all verticals but so far all real-life deployments of universAAL are related to smart living environments. First R&I deployments in Robotics and Smart City domains are also arising.	universAAL is provided under the Apache Software License 2.0, which explicitly guarantees that there are no hidden patents and any existing patent is included in the distribution royalty-free with unlimited usage rights, including commercialization by third parties.

IoT OSS Initiatives	Scope	Domain	Application Areas	IPR Policy
		hence, it is actually a in the B2B sector), but all real-life deployments of universAAL so far are related to smart living environments and hence, some companies are trying to package it with a set of such applications and sell the package in the B2C market; but such packages go beyond the pure open source platform software.		
Warp10 from Citizen Data	Applications knowledge area:	B2B. Applications level. However, it is the generic and technical side of applications level. Not the business application or the user application level.	• Totally generic for IoT Data. • Warp10 allows to build up a real data infrastructure.	Free.

Source: *Compiled by authors*

Appendix 4: Membership fees and Membership class offered by select SDOs

<table>
<tr><th>IoT Alliances/ Consortia / Standard Bodies</th><th>Membership/ Partnership</th><th>Membership fees (Annual)</th></tr>
<tr><td rowspan="3">3GPP (3rd Generation Partnership Project)</td><td>For full membership of 3GPP, an organization must be a member of one of the 3GPP Organizational Partners. these member organizations are called "Individual Members".</td><td rowspan="3"></td></tr>
<tr><td>Guest Membership : Guest status applies to organizations (companies, government departments, educational establishments, etc.) and not to individual people.</td></tr>
<tr><td>Different categories of partnership are also possible: Organizational Partners, Market Representation Partners or Observers.</td></tr>
<tr><td rowspan="2">AVNU Alliance</td><td rowspan="2">There are two levels of membership in Avnu Alliance: Promoter Member and Adopter Member.</td><td>Promoters : $10,000.00</td></tr>
<tr><td>Adopters: $5,000.00</td></tr>
<tr><td rowspan="3">ETSI (European Telecommunications Standards Institute)</td><td>Full membership for organizations established in a country within the CEPT area[238]</td><td>The cost of the first unit of contribution is €6 000 ($ 6612.87) (except for universities, public research bodies, not-for-profit user associations and Micro-Enterprises). The cost of each additional unit is €3,380 ($3725.25)</td></tr>
<tr><td>Associate membership for organizations established in a country outside the CEPT area</td><td>SMEs, user and trade associations, additional membership: €6 000 ($ 6612.87), Micro-Enterprises:€3 000, universities, public research bodies and not-for-profit user associations:€3 000 ($3306.76)</td></tr>
<tr><td>The class of contribution of governmental organizations, in the Member category "Administration[239]"</td><td>The fee is determined by the latest published or available figure of the gross domestic product (GDP) of their country.</td></tr>
</table>

[238] Members' and associate members' contributions are calculated by class. The class is derived from the member company's annual ECRT band. Each class corresponds to a number of units of contribution. This number determines the contribution payable. It also determines the voting weight of a member in ETSI.

[239] *Note that the vote of a national delegation may be cast only if an ETSI full member in the category Administration, Other Governmental Body or National Standards Organization contributes to ETSI according to the GDP.*

IoT Alliances/ Consortia / Standard Bodies	Membership/ Partnership	Membership fees (Annual)
	Observers	Observer membership with limited access rights for organizations in any country. For observers there is a flat rate fee of €4 000 ($4409.02) per year.
Global Platform	Full Membership	$33,000
	Participating	$26,500
	Observer	$13,000
	Public Entity	$7,000
	Consultant	$1,500
GS1		The first-year cost of obtaining a GS1 Company Prefix ranges from $250 for 10 products to $10,500 for 100,000 products[240].
GSMA (GSM Association)	Associate Membership[241]	Range between USD 13,000 to USD 124,000
	Operator Membership	open to licensed mobile network operators using a GSM family technology. Each Member is assigned to one of the 8 Tiers based on the number of its wireless connections and its wireless revenue.
IEC (International Electro technical Commission)	Full members[242]	IEC members are National Committees (NCs) and there can only be one per country.
	Associate Members[243]	
IEEE Standards Association	Professional and students	Professional : US$158.00; Students : US $27
IETF (Internet Engineering Task Force)		There is no membership in the IETF. Anyone may register for a meeting and then attend.

240 Each year after that, there is an annual license renewal fee which allows continued use of the unique prefix number. Annual license renewal fees range from $50 to $2100

241 open to companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in industry sectors such as financial services, healthcare, media, transport and utilities. The annual contribution for Associate Members is based on a company's annual revenue in the previous year.

242 National Committee has access to all technical and managerial activities and functions, at all levels of the IEC, including voting rights in Council.

243 National Committee has full access to all working documents but limited voting rights in the technical work and no eligibility to managerial functions within the IEC.

IoT Alliances/ Consortia / Standard Bodies	Membership/ Partnership	Membership fees (Annual)
International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T)	Sector Member	31,800 CHF ($31864.55). Organizations in a few low income countries benefit from a special reduced fee: 3,975 CHF ($3983.07) per year.
	Associate	10,600 CHF ($10,621.52).
	Academia	3,975 CHF. Academia in developing countries benefit from a special reduced fee: 1,987 CHF ($ 1990.78)per year.
(ISO/IEC) JTC1/WG10 Internet of Things	ISO Member or IEC National Committee	
OCF (Open Connectivity Foundation)	Diamond Member[244]	$350,000 USD
	Platinum Member[245]	Tiered from $5,000 to $50,000 USD
	Nonprofit Educational Gold Member	$1,000 USD
	Basic Member	No fees
OneM2M	Member or Partner	Partner Type 1 organizations (ARIB, ATIS, CCSA, ETSI, TIA, TSDSI, TTA, TTC).
OSGi Alliance	Strategic Member	Organisation with 250 or more Individual : US $25,000 per year; Organisation with less than 250 or more Individual : US $25,000 per year
	Principal Member	Organisation with 250 or more Individual : US $20,000 per year; Organisation with less than 250 or more Individual : US $10,000 per year
	Contributing Associate	US $5,000 per year

244 Diamond Member requires 3/4 affirmative vote of current Directors appointed by Diamond Members.

245 Platinum member is determined by the number of full time employees of the Applicant at the time of application and subject to change on renewal based upon changes in the number of full time employees)

IoT Alliances/ Consortia / Standard Bodies	Membership/ Partnership	Membership fees (Annual)
TMForum	Corporate membership[246]	Range between Corporate A1 annual revenues > $40 billion USD: $150,000 to Corporate E annual revenues < $1 million USD : $2,000
WWRF (Wireless World Research Forum)	Individual Members	100 Euro ($110.20)
	Associate Members:	250 Euro ($275.50)
	Full Members	1.200 Euro ($1322.41)
	Sponsor Members	12.000 Euro ($13224.06)

Source: Compiled from websites of SDOs, consortia's and alliances

Appendix 5: Understanding Compliance of SDOs and Alliances

IoT Alliances/ Consortia / Standard Bodies	Not Managed	Having compliance testing process (include test suites, method, etc.)	Formal certification process
3GPP (3rd Generation Partnership Project)			
AVNU Alliance			
The European Smart Energy Solution Provider (ESMIG)			
ETSI (European Telecommunications Standards Institute)			
Global Platform			
GS1			
GSMA (GSM Association)			
IEC (International Electro technical Commission)			
IEEE Standards Association			

[246] categories are based on your company's total annual revenues reported in your last fiscal year.

IoT Alliances/ Consortia / Standard Bodies	Not Managed	Having compliance testing process (include test suites, method, etc.)	Formal certification process
International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T)		Having compliance testing process (according to the particular specification). No process implemented yet for any IoT related specification	
OCF (Open Connectivity Foundation)			
OneM2M			
TMForum			
WWRF (Wireless World Research Forum)			

Source: Compiled by authors from Alliance for Internet of Things Innovation (AIOTI) 2019

Appendix 6: Solutions offered by B & R Industrial Automation

B&R Industrial Automation, a member of the ABB group is an innovative automation company with headquarters in Austria and offices all around the world. As a global leader in industrial automation, B&R's Industrial IoT solutions offer advantages for both new machinery and equipment (greenfield) as well as existing legacy systems (brownfield) in three main areas: optimize asset utilistion, add sales potential and optimize services. Some of the solutions offered by B&R includes:

- **APROL PDA**: In order to continue raising productivity and lowering maintenance costs, machinery and production plants must be connected in increasingly dense networks. APROL PDA seamlessly captures operational and production parameters such as environmental conditions, quantities, power consumption, duration, waste and more that helps operators analyse the recorded data and implement appropriate corrective measures

- **Orange Box:** Advanced analytics for brownfield assets - As an Industrial IoT solution package, the Orange Box brings smart-factory intelligence to brownfield installations. It is now possible to read and analyse data from previously isolated machinery and equipment.

- **Digital remote access**: With B&R's remote maintenance solution, a service technician can access machines from any - where in the world to retrieve logbook entries, application data and much more. This is done via a certificate-secured and encrypted VPN connection between the SiteManager on the machine and the GateManager at the machine manufacturer's service centre. With the B&R remote maintenance solution, a technician can connect, run diagnostics, adjust parameters and also resolve the errors.

- **Edge Architectures / Cloud connectivity:** B&R edge devices continuously exchange data with IT infrastructure or an external cloud solution. Combine heterogeneous data sources to leverage big data analysis. B&R system solutions offer fully integrated solutions to connect with any cloud service provider using open communications standards such as OPC UA, MQTT, AMQP.

- **Asset Performance Monitor:** Asset Performance Monitor is B&R's first cloud application based on ABB AbilityTM, ABB's unified, cross-industry offering of digital solutions. By giving OEMs a reliable overview of all their machines in the field, it allows them to identify potential improvements, take service operations to the next level and unlock new business models and revenue streams.

- **APROL CONMON:** B&R offers condition monitoring as a pre-installed, pre-configured package that makes implementing predictive maintenance more straightforward. Condition monitoring allows to forecast and plan service more efficiently to maximize machine's uptime.

- **Predictive Maintenance:** B&R solutions helps to detect impending damage before it occurs. In addition to preventing revenue loss, predictive maintenance extends the life of the machine and even opens up new business models.

- **Digital Twin:** B&R supports model-based development at whatever level of detail it is implemented – with modeling, simulation and virtual commissioning woven into its entire product portfolio.

- **APROL ENMON:** B&R's energy monitoring package allows to measure, record and analyze energy consumption to support continuous improvement process. Calculate and improve the effectiveness of individual axes or entire plant. Configure automated reactions to optimize consumption.

- **Open Communication:** The ideal communication protocol for Industry 4.0 - Making IT / OT convergence a reality. OPC Unified Architecture (OPC UA) is a vendor-independent communication protocol for industrial automation applications. Since OPC UA is flexible and completely independent, it is regarded as the ideal communication protocol for the implementation of Industry 4.0.

- **Adaptive manufacturing:** ACOPOStrak and SuperTrak is a revolution in adaptive manufacturing. This highly flexible transport system extends the economy of mass production down to batches of one. B&R's versatile industrial transport systems let you move products through your production line more efficiently while simultaneously improving quality.

- **Mapp Technology**: B&R's Mapp Technology software package helps in collecting data with application-specific software blocks. Data is preselected based on relevance, then recorded and processed in high quality. This provides the perfect foundation for highly effective analysis

Appendix 7: Pan City Components Inventory Proposed under SCP by the 20 Winning Cities in Round 1

S.no	Component	Cities	Count
1	Centralised command and control centre	Bhubaneshwar, Surat, Kochi, Ahmedabad, Jabalpur, Visakhapatnam, Davanagere, Indore, Coimbatore, Belagavi,Udaipur, Ludhiana, Bhopal	13
2	Transit operations system (maintenance and tracking)	Bhubaneshwar, Pune, Jaipur, Ahmedabad, Indore, Solapur, Davanagere, Indore, Kakinada, Udaipur, Guwahati	10
3	Smart parking system	Bhubaneshwar, Pune, Jaipur, Davanagere, Indore, Coimbatore, Kakinada, Udaipur, Guwahati, Chennai, Bhopal	11
4	Common card (payment and operations)	Bhubaneshwar, Jaipur, Surat, Ahmedabad, Indore, Udaipur, Guwahati	7
5	Area based traffic control	Bhubaneshwar, Pune, Ahmedabad, Davanagere, Indore, Coimbatore,	7
6	leak identification system (SCADA/ and AMR)	Pune, Ahmedabad, Solapur, NDMC, Kakinada, Udaipur	6
7	Platform for citizen engagement and all citizen services; city dash board	Kochi, Visakhapatnam, Solapur, Davanagere, Indore, Bhopal	6
8	Traffic mobile app	Pune, Jaipur, Ahmedabad, Indore, Guwahati	5
9	Smart metering (water)	Pune, Kochi, Vizag, Solapur, NDMC, Coimbatore, Belagavi, Udaipur	8
10	CCTV surveillance	Pune, Ahmedabad, Devangere, Indore, Coimbatore, Guwahati, Bhopal	7
11	Emergency response	Bhubaneshwar,Surat, Ahmedabad, Visakhapatnam, Coimbatore, Udaipur	6
12	Public Information system	Pune, Ahmedabad, Davanagere, Indore,	4
13	Public transit and traffic operations and mangement centre	Jaipur, Surat, Ahmedabad,Devangere, Vizag, Indore, Belagavi, Udaipur	8
14	GPS tracking and optimisation of routes of garbage trucks	Jaipur, Jabalpur, Indore, Kakinada	4
15	Wifi- IT connectivity	Pune, Surat, Kochi, Coimbatore, Belagavi, Guwahati	6
16	NMT infrastructure	Devanagere, Belagavi, Udaipur, Guwahati, Chennai, Bhopal	6
17	LED street lighting	Coimbatore, Guwahati, Chennai, Bhopal	4
18	Traffic analysis or roads and video surveillance inside bus using CCTV surveillance	Pune, Indore, Kakinada	3
19	Mobile app based SWM and cleanliness monitoring	Jaipur, Jabalpur, Indore	3
20	Fleet management system	Jaipur, Ahmedabad, Indore,	3

S.no	Component	Cities	Count
21	Automatic fare collection system (transport)	Bhubaneshwar, Jaipur, Surat, Ahmedabad, Indore,	5
22	Variable message sign boards	Ahmedabad, Indore, Bhopal	3
23	Optical fibre enabled communication	Ahmedabad, Indore, Bhopal	3
24	Pedestrian infra	Belgavi, Udaipur, Guwahati	3
25	Smart bulk metering at WTPs	Pune, Surat, Kochi	3
26	24x 7 water supply	Pune,NDMC, Belagavi	3
27	Grievance redressal through web, app and phone	Pune, Vizag, Kakinada, Chennai, Bhopal	5
28	SWM operations and management centre/ system	Jaipur, Jabalpur, Indore, Belagavi	4
29	Smart card for all service payments	Surat, Ahmedabad, Kochi, Indore,	4
30	Smart Bus stops	Pune,Jaipur, Devanagere, Belagavi	4
31	Smart meters for electricity	NDMC, Udaipur	2
32	Solar power capacity implementation	NDMC, Belagavi, Guwahati	3
33	e-healthcare	Vizag, NDMC, Coimbatore, Kakinada	4
34	Air quality monitoring sensors	NDMC , Coimbatore, Bhopal	3
35	City buses	Bhubneshwar, Pune, Devangere, Udaipur, Guwahati	5
36	Hydraullic information system/ flood monitoring	Guwahati, Chennai	2
37	In-bus information system and Wi-Fi	Pune	1
38	Private bus aggregator	Pune	1
39	Intelligent road asset management	Pune	1
40	Give up water subsidy campaign	Pune	1
41	ICT enabled billing and recovery department	Pune, Surat	2
42	e-challans for traffic violations	Bhubneshwar, Pune	2
43	ICT and social media based 2 way communication with citizens	Jaipur	1
44	ERP with GIS platform for corporation	Surat	1
45	Ticket vending machines and value machines	Ahmedabad	1
46	Water accounting at community level	Ahmedabad	1
47	RFID tags for SWM	Jabalpur, Coimbatore, Bhopal	3
48	Street sweeping and dusting machines	Jabalpur	1

S.no	Component	Cities	Count
49	Capacity building of staff	Jabalpur, Ludhiana	2
50	Institutionalising SLB	Solapur	1
51	Mapping of utilities	Solapur	1
52	Data analytics centre	Solapur, Coimbatore, Bhopal	3
53	Intelligent solar powered lights	Devanagere, Belgavi	2
54	Bicycle pods with PIS	Devanagere	1
55	Smart paving (capture energy from movement)	Devanagere	1
56	One website, app and call centre	Devanagere	1
57	Pedestrian and bicycle activated signals	Indore	1

Source: *http://smartcities.gov.in/content/smart_solution.php*

Appendix 8: Pan City Components Inventory Proposed Under SCP by The 13 Winning Fast Track Cities

Sl.	Component	Cities	Count
1	City Navigation System	Port Blair	1
2	Property Survey	Port Blair, Raipur	2
3	GIS	Port Blair, Bhagalpur, Raipur, New Town Kolkata	4
4	Aadhaar Seeding	Port Blair, Raipur	2
5	Emergency Services/ Disaster Management	Port Blair, Bhagalpur, Raipur, Imphal, New Town Kolkata	5
6	CCTV Surveillance	Bhagalpur, Chandigarh, Raipur, Ranchi, Imphal, Warangal, Lucknow, New Town Kolkata, Faridabad	9
7	Command Control Centre	Port Blair, Bhagalpur, Chandigarh, Raipur, Panaji, Ranchi, Imphal, Warangal, Lucknow, New Town Kolkata, Faridabad	11
8	Data Centre	Bhagalpur, Chandigarh, Imphal,	3
9	e-Governance	Port Blair, Chandigarh, Raipur, Imphal, Lucknow, New Town Kolkata	6
10	City Asset Management System	Imphal	1
11	Document Management System	New Town Kolkata	1
12	Wi-fi	Port Blair, Imphal, Agartala, Lucknow, New Town Kolkata	5

Sl.	Component	Cities	Count
13	Optical Fibre	Imphal, Warangal, Agartala, New Town Kolkata	4
14	NMT	Panaji, Lucknow, New Town Kolkata, Faridabad	4
15	Traffic Management System	Bhagalpur, Chandigarh, Raipur, Panaji, Ranchi, Imphal, Shillong, Warangal, Agartala, Lucknow, Faridabad	11
16	Buses/ Fleet Management	Bhagalpur, Raipur, Panaji, Shillong, Warangal, Faridabad	6
17	e-Bus	New Town Kolkata	1
18	Toll Collection	Bhagalpur, Raipur	2
19	e-challan	Bhagalpur, Raipur, Imphal, Faridabad	4
20	Smart Parking	Bhagalpur, Raipur, Panaji, Ranchi, Imphal, Shillong, Warangal, Lucknow, New Town Kolkata, Faridabad	10
21	Vehicle Tracking - Buses/Autos/e-rickshaws	Bhagalpur, Chandigarh, Raipur, Panaji, Ranchi, Warangal, Agartala, New Town Kolkata, Faridabad	9
22	Passenger Information System	Bhagalpur, Raipur, Ranchi, Warangal, Agartala, New Town Kolkata, Faridabad	7
23	Common Smart Card/ Fare Collection System	Raipur, Ranchi, Shillong, Warangal, Agartala, Lucknow, New Town Kolkata	7
24	Road Signage	Bhagalpur, Imphal, Agartala	3
25	Air Pollution Monitoring	Raipur, Panaji, Ranchi, Faridabad	4
26	Solid Waste Management	Bhagalpur, Raipur, Panaji, Imphal, Shillong, New Town Kolkata	6
27	Sewerage	Agartala,	1
28	SCADA – Power	Chandigarh	1
29	Solar Farm/ Solar City	Agartala, New Town Kolkata	2
30	Street Lighting	Lucknow, New Town Kolkata	2
31	Solar Panels	Imphal	1
34	Digital Employment Exchanges	New Town Kolkata	1
35	Incubation Centres	New Town Kolkata	1
37	Telemedicines & Kiosks	New Town Kolkata	1

Source: *http://smartcities.gov.in/content/smart_solution.php*

Appendix 9: List of Smart Cities Standards Developed by International and National Bodies

9.1 ISO standards on Smart Cities

- **ISO 37120:** Sustainable development and resilience of communities –One of the key standards and an important step in this regard was ISO 37120:2014 under the ISO's Technical Committee 26815, providing clearly defined city performance indicators (divided into core and supporting indicators) as a benchmark for city services and quality of life, along with a standard approach for measuring each for city leaders and citizens[247].

- **ISO/TR 37150 and ISO 37151** - This is a technical report on Smart Urban Infrastructures around the world, which serves as a base for the development of the future ISO 37151 standards on harmonised metrics for benchmarking smartness of infrastructures. Some of the indicators include: Smart Cities, Smart Grid, Economic Resilience, Green Buildings, Political Resilience, Protection of biodiversity, etc.[248].

- **ISO/TR 37150:2014** Smart community infrastructures -- Review of existing activities relevant to metrics: ISO/TR 37150 reviews relevant metrics for smart community infrastructures and provides stakeholders with a better understanding of the smart community infrastructures available around the world to help promote international trade of community infrastructure products and give information about leading-edge technologies to improve sustainability in communities

Apart from the standards mentioned above, there are other standards in ISO, which can be linked to a city's environment but are outside the purview of TC 268, such as: ♣ ISO 15686- Buildings and Construction Assets ♣ ISO 13153- Framework and Design Process for Energy Saving Single Family Residential and Small Commercial Buildings ♣ ISO 14001- Environmental Management System ♣ ISO 50001– Energy Management System ♣ ISO 27001- Information Security Management ♣ ISO 20121- Sustainable Events[249]

9.2 IEC Work on Smart Cities

- TC 8 Systems aspects for electrical energy supply - transmission and distribution networks and connected user installations.
- TC8/SC8A grid integration of large-capacity RE generation
- TC 82 Solar photovoltaic energy systems o TC 88 Wind turbines

[247] The World Council on City Data (WCCD)- a sister organization of the GCI/GCIF- was established in the year 2014 to operationalize ISO 37120 across cities globally. The standards encompass 100 indicators developed around 17 themes to support city services and quality of life, and is accessible through the WCCD Open City Data Portal which allows for cutting-edge visualizations and comparisons.

[248] The complete list can be viewed here: http://resilient-cities.iclei.org/fileadmin/sites/resilientcities/files/Webinar_Series/HERNANDEZ_-_ICLEI_Resilient_Cities_Webinar__FINAL_.pdf

[249] Reconceptualising Smart Cities: Centre for Study on Science Technology and Policy

- TC 57 Power systems management and associated information exchange - communications between equipment and systems in the electric power industry
- TC 118 Smart grid user interface - information exchange for demand response and connecting demand side equipment and/or systems into the Smart Grid
- TC 65 Industrial-process measurement, control and automation
- TC 21 Secondary cells and batteries
- TC 105 Fuel Cells technologies
- TC 120 Electrical Energy Storage Systems

Source: Compiled from White Paper on 'Orchestrating Infrastructure for Sustainable Smart Cities[250]'

9.3 Country led standards/ initiatives on Smart Cities

Country	Standards on Smart Cities
British Standards Institution (BSI) UK	Smart city terminology (PAS 180) Smart city framework standard (PAS 181) Data concept model for smart cities (PAS 182) Smart city overview document (PD 8100) Smart city planning guidelines document (PD 8101) BS 8904 Guidance for community sustainable development provides a decision-making framework that will help setting objectives in response to the needs and aspirations of city stakeholders BS 11000 Collaborative relationship management BSI BIP 2228:2013 Inclusive urban design - A guide to creating accessible public spaces.
AENOR , Spain	UNE 178301 on Open Data evaluates the maturity of open data created or held by the public sector so that its reuse is provided in the field of Smart Cities. UNE 178303 establishes the requirements for proper management of municipal assets. UNE-ISO 37120 which collects the international urban sustainability indicators. Following the publication of these standards, 12 other draft standards on Smart Cities have just been made public, most of them corresponding to public services such as water, electricity and telecommunications, and multiservice city networks.
China	When building smart cities, the country will adhere to the ISO 37120 and by the year 2020, China will establish 50 national standards on smart cities

250 https://www.iec.ch/whitepaper/smartcities/

Country	Standards on Smart Cities
Germany	Member of European Innovation Partnership (EIP) for Smart Cities and Communities DKE (German Commission for Electrical, Electronic & Information Technologies) and DIN (German Institute for Standardisation) have developed a joint roadmap and Smart Cities recommendations for action in Germany. Its purpose is to highlight the need for standards and to serve as a strategic template for national and international standardisation work in the field of smart city technology.
Poland	A coordination group on Smart and Sustainable Cities and Communities (SSCC) was set up in the beginning of 2014 to monitor any national standardisation activities. GT 1-2 on terminology and Technical Bodies in PKN Its scope covers a collection of English terms and their Polish equivalents related to smart and sustainable development of cities and communities to allow better communication among various smart city stakeholders. GT 3 for gathering information and the development and implementation of a work programme Its scope includes identifying stakeholders in Poland, and gathering information on any national "smart city" initiatives having an impact on environment-friendly development, sustainability, and livability of a city.
Europe	In 2012, the European standardisation organizations CEN and CENELEC founded the Smart and Sustainable Cities and Communities Coordination Group (SSCC-CG), which is a Coordination Group established to coordinate standardisation activities and foster collaboration around standardisation work
Singapore	In the year 2015, SPRING Singapore, the Infocomm Development Authority of Singapore (IDA) and the Information Technology Standards Committee (ITSC), under the purview of the Singapore Standards Council (SSC), have laid out an Internet of Things (IoT) Standards Outline in support of Singapore's Smart Nation initiative. Three types of standards - sensor network standards, IoT foundational standards and domain-specific standards - have been identified under the IoT Standards Outline

Source: *Compiled from Centre for Internet and Society. https://cis-india.org/internet-governance/blog/database-on-big-data-and-smart-cities-international-standards#_ftn38*

Appendix 10: Cross- Country Comparison: IoT Policies and Focus on Standards

10.1 Bureau of Indian Standards (BIS) Technical Committees: IoT and other related technology standards

LTD 27	**Internet of Things and Related Technologies**
LTD 28	Smart Infrastructure
LTD 29	Block chain and Distributed Ledger Technologies
LTD 30	Artificial Intelligence
LTD 31	Cloud Computing, IT and Data Centres
LTD 32	Biometrics

LTD 33	Wearable Electronic Devices and Technologies
LTD 34	Smart Manufacturing Sectional Committee

Compiled from BIS Website: https://www.services.bis.gov.in:8071/php/BIS/PublishStandards/published/subcommtt?depid=NjY%3D

10.2 Technical References developed by Singapore's IMDA and ITSC's IoT Technical Committee

Standard	Description
TR 38: 2014 Sensor network for smart nation (public areas)	Provides guidance on the communication and application interface standards for the development and deployment of sensor network(s) for public areas in Singapore.
TR 40: 2014 Sensor networks for Smart Nation (homes)	Provides the framework and a minimum set of communication and application interface standards for the development and deployment of sensor networks for homes in Singapore.
TR 47: 2016 IoT reference architecture for Smart Nation	Recommends a minimum set of coherent international or industry standards for interface interoperability of information and services that support a variety of applications across multiple industries and are suitable for deployment on a nation-wide scale.
TR 50: 2016 IoT information and services interoperability for Smart Nation	Provides a Technology-independent reference architecture in support of the development of specific architectures for applications or systems for IoT or sensor networks which are interoperable with each other through a set of well-defined interfaces to achieve seamless data exchange and information use.
TR 64: 2018 Guidelines for IoT security for smart nation	Introduces the foundational security concepts and terminology for Internet of Things (loT) systems and demonstrates their applications. A holistic approach for identifying and mitigating the threats and vulnerabilities of loT systems is also introduced. Guidance is provided on how to conduct threat modelling for loT. In addition, it identifies four basic loT security design principles and demonstrates their applications. Guidance is also provided on how to classify loT security requirements and their usefulness in supporting the identification of security requirements.
IMDA IoT Cyber Security Guide (2019)	A practical guide for enterprise users intending to deploy IoT solutions as well as for their vendors, by providing baseline recommendations, foundational concepts and checklists, focusing with focus on the security aspects for the acquisition, development, operations and maintenance of IoT systems. It builds on the concepts introduced in ITSC TR 64: "Guidelines for IoT security for smart nation" and provides further details on the implementation of IoT security through case studies

Compiled from IMDA & ITSC websites: https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Internet-of-Things

https://itsc.imda.gov.sg/standards/singapore-it-standards/

10.3 EU IoT Regulations

Category	Regulations and Policies
Regulation relating to electronic communications networks and services	European Electronic Communications Code (EECC); net neutrality (part of the Connected Continent Legislative Package), Roaming Regulation and ePrivacy Directive.
Horizontal law and regulation	The Regulation on the free flow of non-personal data, Cybersecurity Act, GDPR, Tangible Goods Directive, Directive on security of network and information systems, Consumer Rights Directive, Product Liability Directive and Unfair Commercial Practices Directive.
Industry-specific regulation	Automotive (e.g. Intelligent Transport Systems Directive, Type Approval Regulation, eCall Regulation), agriculture (Common Agricultural Policy), energy (e.g. Energy Performance of Buildings Directive), aviation (EU Basic Regulation for Drones) and healthcare (Medical Devices Directive).

Cited from *Vodafone's White Paper: A new IoT regulatory framework for Europe*

Indian Council for Research of International Economic Relations (ICRIER)

Research Location

Plot No. 16-17, Pushp Vihar, Institutional Area, Sector 6, New Delhi-110017
(91-11) 43 112400
(91-11) 24620180

Seminar and Outreach

Core 6A, 4th Floor India Habitat Centre, Lodhi Road, New Delhi 110003