सत्यमेव जयते

TEC INITIATIVES IN M2M/ IoT DOMAIN

An overview

TEC 31198:2022

ISO 9001:2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA

RELEASE 2.0

Updated in June, 2023

Revision History

Date	Release	Document No.	Description
March, 2022	R1.0	TEC 31198:2022	TEC Initiatives in M2M/ IoT domain- *An overview*
June, 2023	R2.0 (superseded R1.0)	TEC 31198:2022	TEC Initiatives in M2M/ IoT domain- *An overview*

Important Notice

Individual copies of the present document can be downloaded from TEC website using link **(https://www.tec.gov.in/M2M-IoT-technical-reports)**
Users of the present document should be aware that the document may be subject to revision or change of status.

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

Table of Contents

Introduction

Internet of Things (IoT) is one of the fastest emerging technologies across the globe, providing enormous beneficial opportunities to society, industry, and consumers. It is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety & Surveillance, Remote Health Management, Agriculture, Smart Homes and Smart Cities etc., using connected devices. IoT is benefitted by recent advances in several technologies such as sensors, communication technologies (Cellular and non-cellular), AI/ ML, Cloud / Edge computing etc.

There may be 26.4 billion IoT devices in service globally by 2026. Out of this, approximately 20% will work on cellular technologies[1].

As per the National Digital Communication Policy (NDCP) 2018[2] released by Department of Telecommunications (DoT), an eco-system is to be created for 5 billion connected devices by 2022.

Government of India declared the names of 100 cities to be developed in phased manner as Smart Cities. Work in most of the cities is in progress by Smart City SPVs created for this purpose. Smart Cities being developed should remain smart not only for the present generation but even for the future generations. For this it is imperative to use standards based solutions enabling smart cities components to be scalable, efficient, cost effective.

Security of IoT eco-system end-to-end i.e. from devices to the applications is very important as the hacking of the devices/networks being used in daily life would harm companies, organisations, nations and more importantly people.

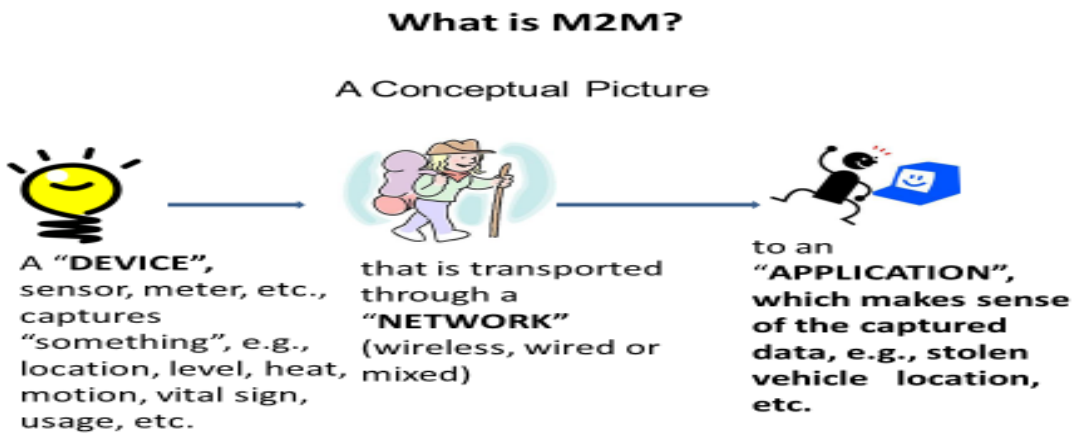
TEC being the national standardization body (NSB) for telecom & ICT sector, participates and submits contributions in various Standards Developing Organisation such as ITU, APT, ETSI, 3GPP, oneM2M, ISO/ IEC JTC1 SC 41 etc. at international level and BIS & TSDSI in India.

TEC has been working in M2M/ IoT domain since 2014 and has taken a number of initiatives. This document provides the summary of TEC works carried out in M2M/ IoT domain.

1. Machine to Machine (M2M) Communication

M2M refers to the technologies that allow wired / wireless system to communicate with devices of same ability. M2M uses a device (sensor, meter etc.) to capture an 'event' (motion, meter reading, temperature etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information.

[1] https://www.ericsson.com/4a03c2/assets/local/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf
[2] https://dot.gov.in/sites/default/files/Final%20NDCP-2018_0.pdf



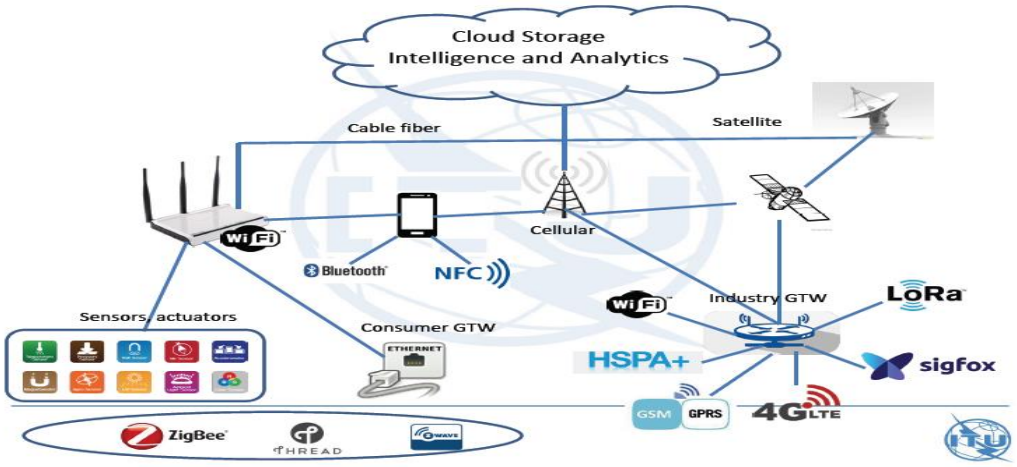
2. Internet of Things

All the computers connected to the Internet can talk to each other. Use of mobile phones for connecting internet has revolutionized the entire scenario. With Internet of Things, the communication is extended via Internet among all the things that surround us.

IoT is benefitted by a number of technologies i.e. M2M communication, Cellular and non - cellular communication technologies, AI/ ML, Cloud computing, edge computing etc.

The IoT ecosystem comprises M2M devices, Gateways, M2M Communication technologies, big data and process management, IoT platform, User interface (web, Mobile, HMI) and end to end security.

ITU has defined Internet of Things (IoT) as "***A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies***"[3].



[3] Source: ITU-T Y.2060 - Y.2060 : Overview of the Internet of things (06/2012) (https://www.itu.int/rec/T-REC-Y.2060-201206-I)

3. M2M / IoT Applications

M2M / IoT technology can make any vertical smart. Some of the verticals and related applications have been mentioned in the table below:

S.No.	Vertical	Vertical related applications
1	Smart City	Intelligent transport System, Waste management, Street Light control system, Water distribution, Smart Parking, Intelligent buildings, Safety & Security
2	Automotive / Intelligent Transport System	Vehicle tracking, e-call (911 in USA, 112 in Europe, India has adopted 112), V2V and V2I applications, traffic control, Navigation, Infotainment, Fleet management, asset tracking, manufacturing and logistics.
3	Utilities / Energy	Smart metering, smart grid, Electric line monitoring, gas / oil / water pipeline monitoring
4	Health Care	Remote monitoring of patient after surgery (e-health), remote diagnostics, medication reminders, Tele-medicine, wearable health devices
5	Education	Tele education, e-attendance (biometric)
6	CCTV based Real time public safety system	Commercial and home security monitoring, Surveillance applications, Video analytics and sending alerts, Fire alarm/ alerts, Police / medical alert
7	Smart Home	Security & alarm, Connected appliances, Smart lighting system
8	Agriculture	Remotely controlled irrigation pump, Crop Management, Soil analysis
9	Smart Manufacturing (Industry 4.0)	Proactive maintenance of machines, Shop floor monitoring, Industry automation
10	Food Processing	Production & Storage, better food safety, wastage reduction
11	Aqua-culture	Water quality (dissolved oxygen, ammonia, pH, etc.) management, intelligent feeding, aquatic animal health management
12	e- Governance	Citizen centric services like birth/death certificate, electronic attendance in government projects, connecting police station, banks, post offices, etc.

4. Challenges in the IoT domain

Some of the important challenges are as given below:

a. **Robust connectivity: -** It is very important for timely transmission of the data. Latency, availability, coverage and cost are some of the factors deciding the appropriate communication technology.

b. **Standardization: -** There is a need for **s**tandards for various elements of the IoT ecosystem to ensure long term sustainable solutions and to prevent vendor lock-in in case of proprietary solutions.

c. **Interoperability and open interfaces: -** Interoperability is required at the device, network and platform/ application levels. Interoperability is important to achieve the economies of scale.

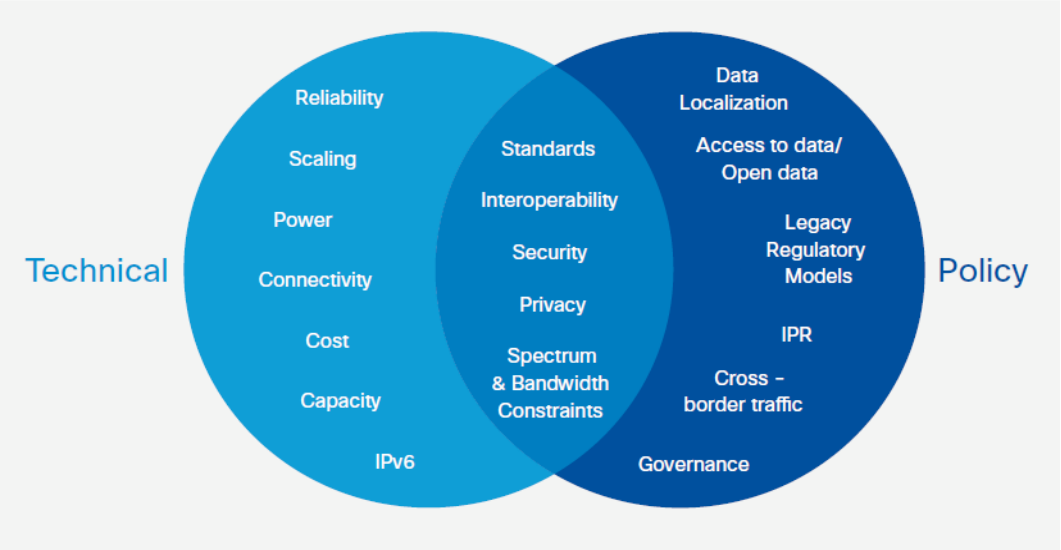
d. **Slow deployment of IPv6:**- All the devices/ gateways to be connected to PSTN/ PLMN are required to have unique address. As IPv4 are going to exhaust, it will be better to migrate to IPv6 as an earliest possible.

e. **Technologies for sustainability/ long life batteries** is required for sensors.

f. **Security of IoT devices/ eco system** is required to build trust in the network and also to manage vulnerabilities.

g. **Privacy** is very important especially in health-care

There is a need to generate indigenous IPR (Intellectual Property Rights) for creation of standards and further contribution in global SDOs. Reliable connectivity, localization of data in cross border traffic, spectrum requirement for low power devices are some of the challenges to be resolved. Following diagram shows the challenges related to technology and policy.



[Source: Harnessing the IoT for Global development, ITU, 2016]

5. Standardization at Global level

A number of international organizations are working on standardization in the IoT domain such as ITU (ITU-T SG-20 on IoT and Smart Cities & Communities, ITU-T SG-17 on Security), ISO/IEC (ISO/IEC JTC1/ SC41 on IoT and Digital Twin and ISO/IEC JTC1/ SC27 on Information security, cyber security and privacy protection), oneM2M, 3GPP, ETSI, IEEE etc.

5.1. ITU-T Study Group -20 (SG-20) & related bodies

ITU-T constituted Study Group 20 (SG-20) on ***IoT and its applications in Smart cities & Communities*** (SC&C) in 2015. SG-20 works for the development of globally harmonized standards on IoT and Smart Cities.

ITU-T SG-20 has released a large range of standards related to city planning, stakeholders' engagement, Devices / Sensors, Gateways, Platforms, Big data, Open data, Smart data Governance, Frontier technologies, Use cases, KPIs for assessing the Smartness of a City etc. Details are available on https://www.itu.int/en/ITU-T/studygroups/2022-2024/20/Pages/default.aspx .

U4SSC: ITU is the founding member of U4SSC (United for Smart sustainable cities), an initiative supported by 16 other UN partners with the aim of achieving SDG goal 11 (make cities inclusive, safe, resilient and sustainable).

U4SSC developed Key Performance Indicators (KPIs) for Smart Sustainable Cities based on ITU standards.

More than 150 cities across the globe are evaluating their progress towards the objective of developing Smart Sustainable Cities and achieving SDGs as well, using these KPIs. (e.g. Dubai, Singapore, Wuxi (China), Moscow (Russia), Valencia (Spain), Pully (Switzerland)). More details are available on https://u4ssc.itu.int/ and also in TEC TR on IoT and ICT Standards for Smart Cities released in 2022 and available on https://tec.gov.in/M2M-IoT-technical-reports .

ISO-IEC-ITU J-SCTF: ITU, ISO and IEC have established a Joint Task Force to coordinate international standardization for smart cities and communities to build synergies in the ongoing work. This task force represents an integrated response towards achieving UN SDG11 'Make cities inclusive, safe, resilient and sustainable goals'. ISO, IEC and ITU have designated experts to work on the agenda items of the task force. ITU-T SG-20 liaisons in this task force on behalf of ITU.

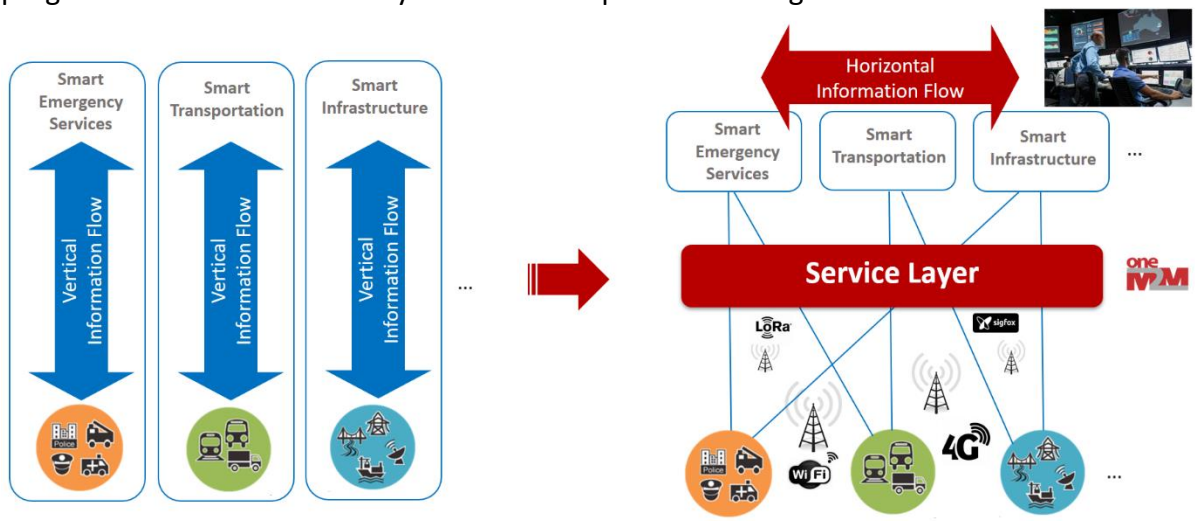
DoT is the member state in ITU and TEC is having the mandate to participate in ITU-T activities. TEC is having National Working Groups in line with ITU-T Study Groups. National Working Group (NWG-20) coordinates and submits contributions in ITU-T SG-20.

5.2. ISO/IEC JTC1 SC41

ISO/IEC joint technical committee (JTC1) subcommittee (SC 41) is working on ***IoT and Digital Twin***. BIS represents India in various committees of ISO/ IEC.

5.3. oneM2M

ETSI (Europe), TTC, ARIB (Japan), ATIS, TIA (USA), TTA (Korea) CCSA (China) had come together and created a partnership project oneM2M, to avoid creation of competing M2M standards. They are working to **create standards for the common service layer**. From India, TSDSI is the member of oneM2M. oneM2M has released first set of specifications in Jan 2015, 2nd in March 2016, 3rd in Dec 2018. Work on 4th and 5th set of specifications is in progress. A common service layer has been depicted in the figure below:



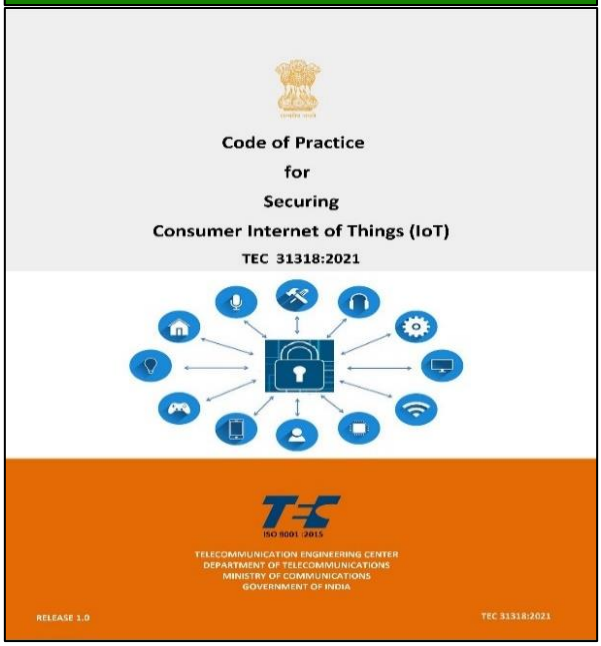
oneM2M Release 4 which is expected to be published in near future is having one of the work items in progress on C-V2X interworking namely ***Vehicular domain support enhancements and 3GPP V2X interworking.***

ITU-T SG-20 has adopted oneM2M Release 2A (Release 2 + some more specifications) specifications. TEC has adopted oneM2M Release 2 and Release 3 specifications as National Standards (details in section 9).

6. Technical Reports (TRs) released in M2M/ IoT domain

TEC started working in M2M/ IoT domain since 2014. TEC formed various multi-stake holders working groups in the last 4 -5 years to study M2M/ IoT domain, having members from academia, OEMs, start-ups, industries, SDOs, Government etc. TEC has released **nineteen Technical Reports**[4]**,** with the outcomes intended to be used in the formulation of policies/ standards.

Total members of all working groups taking together may be around 150.



1. M2M Enablement in Power Sector
2. M2M Enablement in Intelligent Transport System
3. M2M Enablement in Remote Health Management
4. M2M Enablement in Safety & Surveillance Systems
5. M2M Gateway & Architecture
6. M2M Number resource requirement and options
7. V2V / V2I Radio Communication and Embedded SIM
8. Spectrum requirements for PLC and Low Power RF Communications
9. ICT Deployments and strategies for India's smart cities: A curtain raiser
10. M2M/ IoT Enablement in Smart Homes
11. Communication Technologies in M2M / IoT domain
12. Design and Planning Smart Cities with IoT/ ICT
13. Recommendations for IoT / M2M Security
14. IoT/ ICT Enablement in Smart Village & Agriculture
15. Code of practice for Securing Consumer IoT
16. Emerging Communication Technologies and use cases in IoT domain
17. IoT/ ICT Standards for Smart Cities
18. Framework of National Trust Centre for M2M/IoT Devices and Applications
19. Security by design for IoT device manufacturers

[4] https://www.tec.gov.in/M2M-IoT-technical-reports

7. Brief about the Technical reports released in the recent years (2021-23)

7.1. Technical Reports related to IoT Security

Background: Based on TRAI recommendations on ***Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications,*** released in Sept 2017, following two work items were communicated by NT Cell DoT to TEC:

> (i). Device manufacturers should be mandated to implement "Security by design" principle in M2M devices manufacturing so that end to end encryption can be achieved.
>
> (ii). A National Trust Center (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software).
>
> *However, for certification of software products & applications related M2M devices, STQC (Standardization Testing and Quality Certification) under Meity (Ministry of Electronics and Information Technology) may be the agency to carry out such testing under single window of proposed National Trust Center.*

To study both the work items, a multi-stake holders working group having members from industries, academia, R&D, SDOs, Government etc. was formed.

Work item mentioned at point number (i) Security by design principles will help in the development of secured IoT device and the work item at point number (ii) is expected to create the trusted IoT devices ecosystem by means of testing and certification. However, the Essential requirements for testing of IoT devices under MTCTE have already been prepared and are available on TEC MTCTE portal.

IoT devices hardware will be tested as per Essential Requirements (ERs) under MTCTE having testing specifications related to EMC, Safety, communication interfaces, IP, SAR and Security. Security specifications being prepared in ITSAR (Indian telecom security assurance requirements) are also the part of ERs. Software of the IoT devices will be tested by STQC.

As a result of study on the above work items, following three technical reports have been released.

7.1.1. Security by design for IoT Device Manufacturers

Technical Report ***Security by design for IoT Device Manufacturers*** (TEC 31328:2023) released in March 2023, highlights various threats and challenges related to IoT device security; includes study of national/ international standards (by ITU, ISO/ IEC, ETSI, ENISA, IoTSF, NIST, GSMA, 3GPP etc.), best practices and guidelines (UK DCMS, CSA Singapore, WEF, STQC etc.) to mitigate these challenges. This report also provides recommendations for IoT device manufacturers and related stakeholders, which will help in securing IoT

ecosystem in the country. Some important standards related to security have been listed in Annexure- I of this report.

7.1.2. Framework of National Trust Centre for M2M/ IoT Devices and Applications

The technical report on ***Framework of National Trust Centre for M2M/ IoT Devices and Applications***[5] visualises the implementation of national trust centre in a phased manner for managing/ addressing the vulnerability related issues of the IoT devices reported by IoT/ Smart city platforms working in the network. This technical report has been released in March 2022.

As the MTCTE is in beginning stage therefore it may take time to have only the certified devices in the network. However, efforts should be made to enhance the share of certified devices in the network in near future.

There will be certified (as per MTCTE) as well as non-certified (already deployed/ not covered in MTCTE) devices in the network.

However, as per study of various global documents and discussion in the working group it has been envisaged that Vulnerabilities may arise from any device working in the network and should be addressed in a time bound manner by manufacturers.

NTC portal is being developed by C-DOT in coordination with TEC/ DoT and NCSC.

7.1.3. Code of practice for Securing Consumer IoT

The report ***Code of practice for Securing Consumer IoT***[6] released in August 2021, provides baseline requirements for securing Consumer IoT, aligned with global standards and best practices. Guidelines available in this report, will be helpful in securing consumer IoT devices & ecosystem as well as managing vulnerabilities. This technical report is based on the guidelines available in ETSI TS 103 645.

This report is intended for the use of IoT device manufacturers, Service provider's / system integrators and application developers etc.

Similar guidelines have been released by UK in 2018, European Union (EU) in 2020, Singapore, Finland, Australia, Vietnam etc.

It is worth mentioning that the IoTSF document ***Contemporary use of Vulnerability disclosure in IoT***[7] released in Nov 2021, has also mentioned this technical report. IoTSF has

[5] https://www.tec.gov.in/pdf/M2M/TR_National%20Trust%20Center_TEC%2031188_2022.pdf
[6] https://tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf
[7] https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf

given a number of recommendations including to mandate the vulnerability reporting as part of regulatory framework.

DoT has issued the Office Memorandum (OM) in July 2022 to all the ministries of Government of India and telecom service providers with the request for wider circulation of TEC technical report on Code of practice for Securing Consumer IoT to all related stakeholders (IoT device manufacturers, IoT Service Providers System Integrators, Application Developers etc.) for voluntary adoption of the guidelines available in this document and provide feedback.

DoT has also issued the OM in March 2023 to M2M service providers to follow the first three guidelines of this technical report.

7.2. IoT/ ICT Standards for Smart Cities[8]

This Technical Report, released in March 2022, has covered the existing policies and guidelines/ standards related to the development of smart infrastructure released by various ministries/ organisations in India as well as some foreign countries namely EU, Japan, Korea, Singapore, Dubai etc. Verticals namely Automotive, Power, City Surveillance, Water management, Waste management and health care have been studied and the related policies and IoT/ ICT based standards / use cases have been have listed. Related Standards released in India by MoRTH, BIS and TEC; and by international SDOs like ETSI, ITU-T SG-20, ISO/IEC JTC1 SC41 have been studied and the important standards have been listed in this document. This technical report is expected to work as a guiding document for Smart City SPVs, Consultants, OEMs and other stakeholders in the development of sustainable Smart Cities.

TEC standards are available in Annexure-5 and recommendations in Section-6 of this report. TEC standards listed in this report may be used in procuring the telecom equipment and Smart devices for the development of Smart Cities.

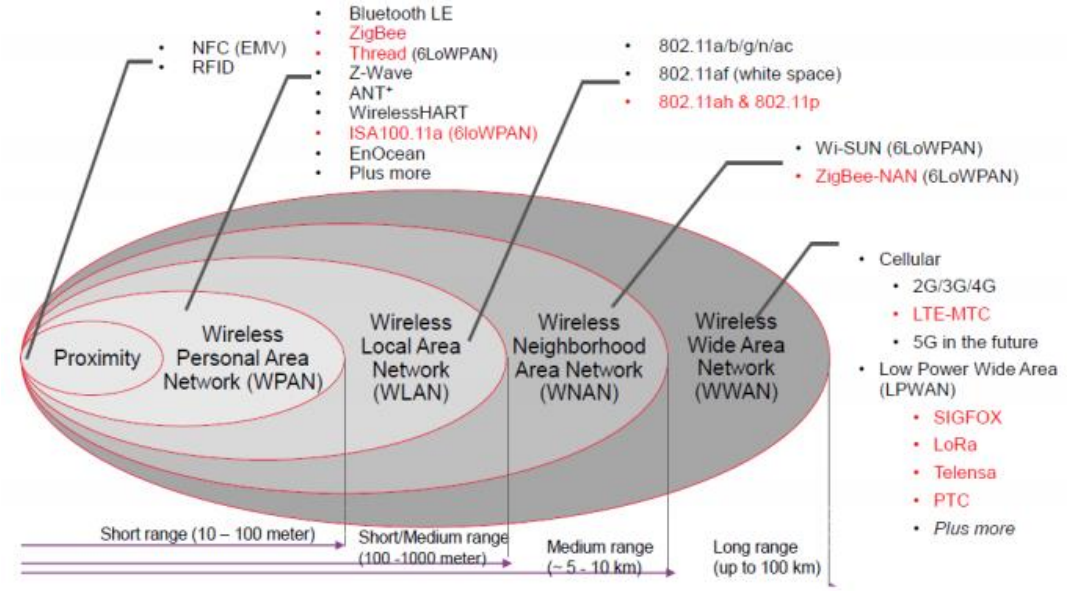
7.3. Communication Technologies and Use cases in IoT domain

Communication technologies play a crucial role in the development of IoT/ Smart Cities for connecting smart devices and transmitting data in real time. Smart Cities may comprise tens of thousands of smart devices in different types of use cases, among which some applications will require high bandwidth (e.g. surveillance cameras) while other may require low bandwidth (e.g. only few Kbps for transmitting data from panic button of a cab/ bus, fire alerts, metering data etc.). Communication technologies for M2M / IoT domain have been studied, resulting in two technical reports, released in 2017 and 2021.

Technical Report released in 2017 on ***Communication technologies in M2M/ IoT domain***[9] *has covered in detail the Cellular Technology (2G, 3G, 4G i.e. up to LTE 3GPP release 14), Low*

[8] https://www.tec.gov.in/pdf/M2M/TR_IoT%20ICT%20Standards%20for%20Smart%20Cities.pdf

power wireless communication technologies (NFC, RFID, Bluetooth, ZigBee etc.), Low power wide area network technologies (LPWAN – cellular/ non-cellular), Wi-Fi [IEEE 802.11 a, b, g, n, ac (variant of Wi-Fi)], DSRC (802.11p), wire line (PLC, DSL, FTTH) etc. and the related use cases.



Due to advancement in technology, further study has been done and the Technical Report on ***Emerging Communication Technologies and Use cases in IoT domain***[10] released in November 2021. This report covers 5G, Wi-Fi 6, WiFi 6E, WiFi HaLow, Bluetooth Mesh and some important use cases such as Intelligent transport system (Connected vehicles, C-V2X etc.), Private Industrial Network (Smart factories, Industry 4.0) , Smart homes etc. **This report provides recommendations on spectrum and regulatory related aspects, which may be quite useful in the development of eco-system in India.**

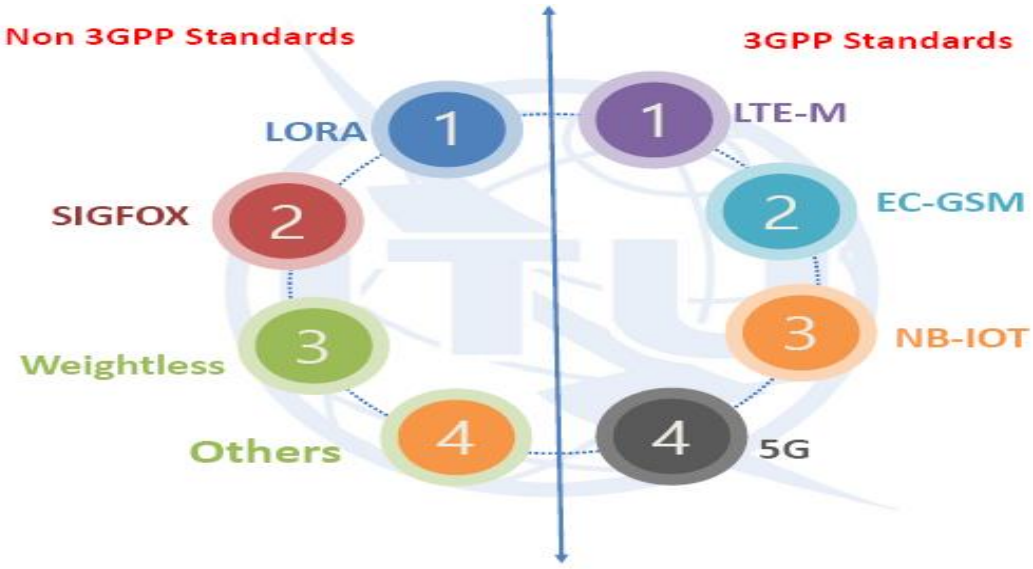
7.3.1 Low Power Wide Area Network (LPWAN) technologies

LPWAN technologies have been developed to carry a very small data to a large distance and consume very low power. It covers 2-3 Km in city (dense) areas and 12-15 Km in rural (open) areas. Expected battery life is around 10 years. LPWAN technologies are available on 3GPP as well as non 3GPP standards, as shown in Figure below.

Use cases: Smart metering (Electricity/ water / gas), Smart farming (transmitting Soil testing data), Smart bin, transmitting pollution sensor data, transmitting fire alerts etc.

[9] https://tec.gov.in/pdf/M2M/Communication%20Technologies%20in%20IoT%20domain.pdf

[10] https://tec.gov.in/pdf/M2M/Emerging%20Communication%20Technologies%20&%20Use%20Cases%20in%20IoT%20domain.pdf

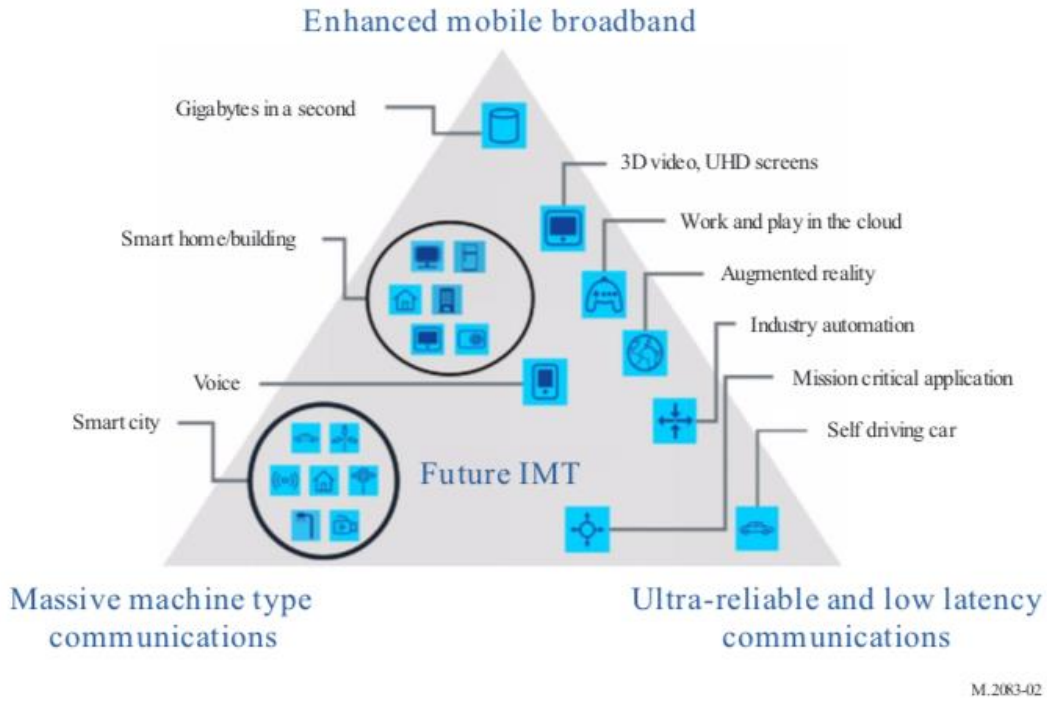


Non-3GPP LPWAN technologies such as LoRa and Sigfox are being deployed across the globe. LoRa and Sigfox networks are deployed in delicensed sub GHz frequency band and in India it is 865-868 MHz. M/s TATA Communications Ltd. (TCL) and M/s SenRa are deploying LoRa based network in India.

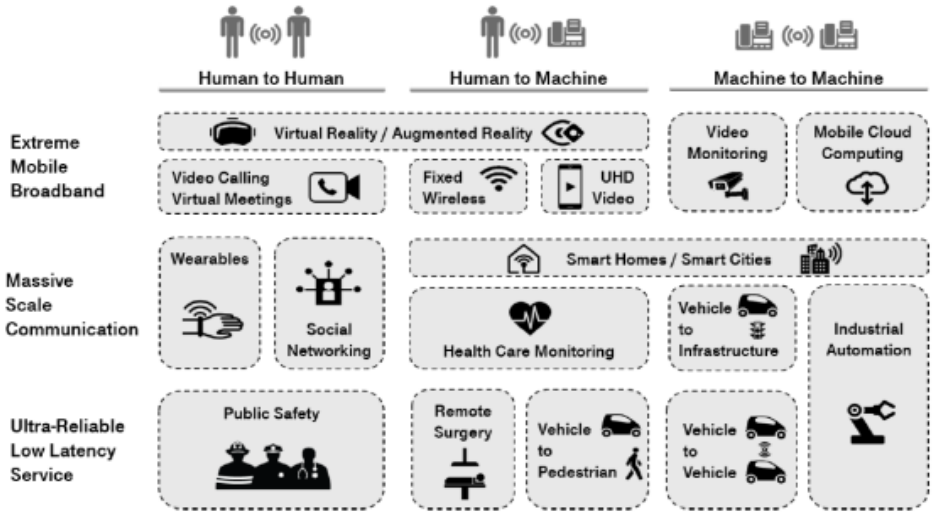
3GPP has already released specifications in its Release 13 and onwards for LPWAN services, which may co-exist in the existing cellular networks. Three variants in LPWAN technologies in cellular domain are EC-GSM, NB-IoT and LTE MTC. Cellular operators may enable LPWAN services in the existing GSM / LTE networks by upgrading the software. Trials are already in progress and the commercial offerings are also available in a number of countries across the globe. Cellular operators in India are also doing trails for providing NB-IoT services.

7.3.2 5G Technology

5G is an emerging communication technology for IoT domain, as it provides features such as enhanced Mobile broadband (Higher data rate: 100x faster, peak data rate – 10 Gbps), Mission critical services (Ultra reliable & low latency communication) such as V2V/ V2I applications, Robotics surgery, Drones etc. and Massive M2M (100x more connected devices). These three features have been depicted in the figure below-



5G is also having the additional important features such as beam forming, small cells, consume less energy than 4G etc. These features are not available in 2G - 4G technologies. Most of these features have already come in 3GPP Release 15 and 16. Work on 3GPP Release 17 is in progress and expected in Q2 of 2022. Some of the use cases related to various features of 5G technology have been shown in figure given below:



[Source: 5G Americas]

5G technology in precision agriculture will ensure greater profitability and efficient utilization of resources by use of automated tractors / harvesters, precision seeders, and automated weed & pest controllers. Drones with 5G technology may be used efficient & precise spraying of fertilizers in fields, and also to scan and identify

unwanted weeds through the use of AI. It will help farmers to better organize and allocate their time and attention towards areas that really need it.

LTE/ 5G based C-V2X technology may be deployed for Intelligent Transport System. 5G features will be quite useful for Industry 4.0 also.

7.3.3 C-V2X [Cellular - Vehicle to everything]

3GPP released LTE C-V2X specifications in its Release 14 in 2017, which establishes the foundation for safety use cases. C-V2X is said to provide not only the direct communication (which DSRC provides) but also the network based communication V2N which can be used to provide network assistance for safety related features. C-V2X employs two complementary transmission modes:

- **Short-range direct communications**
  - Vehicle - to – vehicle (V2V) for collision avoidance safety system etc.,
  - Vehicle – to - Infrastructure (V2I) for traffic signal timing / priority etc.
  - Vehicle - to - Pedestrian (V2P), such as cyclists and pedestrians for safety alerts etc.

In this mode, C-V2X works independently of the cellular networks in dedicated Spectrum in 5.9 GHz band.

- **Long-range network communications**
  - **Vehicle – to – network (V2N) for** real time traffic routing / cloud services, in which C-V2X employs the conventional mobile network to enable a vehicle to receive information about road conditions and traffic in the area, beyond the driver's line of sight.

- **C-V2x specifications published by 3GPP are listed below:**

  - LTE based C-V2X, as specified in 3GPP Release 14 (published in 2017), and Release 15 (published in 2018).
  - Applications and protocols developed by SAE.

3GPP Release 14 (published in 2017) specifications for LTE based C- V2X provide improvements over 802.11p / DSRC technology for active safety use cases and beyond. 3GPP Rel 15 (published in 2018) provides further improvement in C-V2X safety, range and reliability.

3GPP Rel-16 (published in 2020) provides specifications for 5G and NR based C-V2X, with continuing evolution path for future releases. 5G NR C-V2x will have backward compatibility with Rel 14 C-V2x.

5G roadmap will further improve the connected vehicle segment built on cellular V2X.

C-V2X Use cases: Some of the important C-V2X Use cases are Forward Collision Warning, Emergency Electronic Brake Lights, Do Not Pass Warning, Left Turn Assist, Intersection Movement Assist, Blind Spot Warning/ Lane Change Warning, Emergency Vehicle Alert, platooning etc.

C-V2X is designed to work in ITS 5.9 GHz spectrum band for vehicles to talk to each other on harmonized dedicated spectrum. C-V2X support in ITS band was added in 3GPP Release 14 published in 2017. V2V, V2I and V2P services require low latency network, therefore operate through RSU (road side units) in 5.9 GHz band and is independent of cellular communication. V2N operates through cellular network.

5GAA (5G automotive association)[11] is a cross industry consortium connecting the vehicle manufacturers and telecom industry to work closely together to develop end to end solutions for future mobility and transportation services. 5GAA has over 130 member companies representing Global automakers, mobile operators, semiconductor companies and test equipment vendors. 5GAA is working on Intelligent transport solutions based on C-V2X technology and a number of trails are already in progress in a number of countries.

Spectrum allocation: C-V2X has widespread support within the mobile and automotive industries. The Federal Communication Commission (FCC) USA has issued a directive in November 2020 to allocate the upper 30 MHz of the 5.9 GHz (5.895 – 5.925) ITS band to C-V2X technology that gives the C-V2X industry the green light to deploy C-V2X Roadside Units (RSU) and Onboard Units (OBU).

The Ministry of Industry and Information Technology China also issued the administrative regulations on the Use of 5.905-5.925 GHz Spectrum for Direct Connected Communication on the Internet of Vehicles, which established dedicated C-V2X spectrum with a total bandwidth of 20 MHz.

The current National Frequency Allocation Plan allows for use of frequency band 5875 – 5925 MHz for Intelligent Transport Networks (IND 30). Suitable spectrum (around 30 MHz) may be allocated for C-V2X in this range.

As the intelligent transport system is an important requirement in India and no technology has been deployed in the past, it will be better to adopt C-V2X technology based on 3GPP specifications.

Intelligent Transport system with C-V2X has been covered in detail in TEC Technical Report on ***Emerging Communication Technologies and Use cases*** in IoT domain.

NITI Aayog floated a policy paper on Intelligent Transport System. TEC provided the comments on technology as well as on policy and submitted to DoT. It was

[11] https://5gaa.org/wp-content/uploads/2021/06/5GAA_S-210019_Position-paper-on-European-deployment-band-configuration-for-C-V2X_final.pdf

also mentioned by TEC that TEC/ DoT and MoRTH should work hand in hand for the development of this ecosystem. Comments were sent to SRI wing, DoT.

7.4. IoT/ ICT Enablement in Smart Village & Agriculture[12]

This technical report released in March 2021, focuses on diverse issues related to IoT/ ICT infrastructure and also in the verticals such as agriculture, animal husbandry, fisheries, healthcare, education, water management etc. in rural areas; resolving these issues by creating telecom infrastructure using OFC of Bharatnet and extending the network through Wi-Fi Hotspots/ Low power wide area network (LPWAN) /mobile BTS for providing smart solutions using IoT devices and Smart phones.

It has also covered a large number of use cases like Remote patient monitoring, Soil nutrients monitoring, Smart irrigation, Animal activity monitoring tag, Arresting food adulteration using IoT & Blockchain, Smart anganwadi, IoT & ML based Smart aquaculture, 5G and Intelligent farming, Drone application in Agriculture and A smart village model etc.

8. Important actionable points emerged from the Technical Reports (TRs) and action taken thereafter

8.1. Actionable points emerged from reports released till 2022 and their implementation

A large number of actionable points have emerged from these technical reports. Some of the important, which are in process at different levels of adoption in policy / standards:

1. **13-digit numbering scheme for SIM based devices/ Gateways**
   As per the recommendation in Technical Report on "M2M Number resource requirement & options", 13-digit M2M Numbering scheme for SIM based devices/ Gateways, which will co-exist with the existing 10-digit numbering scheme in use, was prepared by TEC.

DoT approved the 13-digit numbering scheme for SIM based devices / gateways in 2016 and issued instructions to the Telecom Service Providers for its implementation in 2018.
Five codes of 3 digit each (559, 575, 576, 579 and 597) have been allotted as a M2M identifier[13].

[12] https://tec.gov.in/pdf/M2M/IoT_ICT%20enablement%20in%20Smart%20Village%20&%20Agriculture.pdf
[13]https://dot.gov.in/sites/default/files/M2M%20numbering.pdf?download=1

2. **M2M SIM / Embedded SIM and remote subscription management**
   Based on the Technical Report on "***V2V / V2I Radio communication and Embedded SIM***", Interface Requirement (IR) has been released by TEC.

   - DoT approved the use of Embedded SIM with OTA provisioning in May 2018[14].
   - Ministry of Road Transport and Highways, India has already included Embedded SIM with OTA provisioning based on TEC specifications in AIS140 standard which specifies the conditions and specifications for the use of connected devices in vehicles[15].
   - The Bureau of Indian Standards has released a new Standard for Automotive Tracking Device and Integrated Systems (IS: 16833/2018) which mandates the use of the embedded SIM as per the Standards/Specifications of the TEC.

3. **Multi-protocol gateway / IoT Gateway**
   It is Important for Smart homes/ building solutions for interconnecting the devices with the communication networks and it performs the necessary translation between the protocols used in the communication networks and those used by devices. Essential Requirement (ER) under MTCTE regime has been approved and available on MTCTE portal.

4. **Additional Spectrum requirement for Low power wireless communication technologies**
   - Based on the Technical Report on "***Spectrum requirements for PLC and Low power RF communications***", additional Spectrum of 12MHz for Low power RF communication technologies in Sub GHz band, adjacent to existing delicensed spectrum (865-867 MHz) was recommended to reserve and release as per requirement.
   - DoT referred the case to TRAI.
   - TRAI had recommended 7 MHz spectrum [1 MHz spectrum in 867- 868 MHz and 6 MHz in 915-935 MHz band] to be delicensed on priority, in its recommendation on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" released in Sept. 2017.
   - DoT approved the TRAI recommendations.
   - 1MHz spectrum has been released adjacent to 865-867MHz increasing it to 865-868MHz vide GSR 853(E) dated 10th Dec 2021.

[14]http://www.dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1
[15]https://hmr.araiindia.com/Control/AIS/14201910518PMAIS-140.pdf

5. **Spectrum Requirement in Power Line Communication (PLC)**

   Based on the Technical Report on "***Spectrum requirements for PLC and Low power RF communications***", It is recommended to allocate a frequency band of 0 - 500 KHz for narrowband PLC, 2 MHz - 200 MHz for broadband PLC and any other band (for narrowband or broadband PLC) on which new technologies may be developed.

6. **Spectrum requirement in 5.9 GHz band for DSRC/ C-V2X technology for Intelligent Transport System in India**

   As per ITU-R Recommendation M.2121, 5850 – 5925 MHz spectrum has been reserved for ITS applications. Same has also been recommended by TEC in its report ***V2V/ V2I Radio Communication and Embedded SIM*** released in 2015 and also in ***Emerging Communication Technology and use cases*** released in 2021. DSRC being an outdated technology at present, C-V2X is expected to be deployed for Intelligent Transport System in India. The current National Frequency Allocation Plan allows for use of frequency band 5875 – 5925 MHz for Intelligent Transport Networks (IND 30). For realizing the full potential of V2X, a unified technology and enabling regulatory provision for a deployment authority is required.

7. **Common service layer at the IoT platform**

   Common service layer concept has been described in detail in TEC Technical Report on ***M2M Gateway & Architecture*****, released in 2015.** It is quite important for sharing of data between various verticals connected at the platform for ensuring interoperability. It will help in breaking silos.

   At present most of the smart cities are using proprietary platforms, therefore two adjacent and different proprietary platforms are not able to share the data in real time. Moreover, these platforms may not be scalable and will be difficult to integrate new services and further innovation.

   oneM2M specifications are having common service layer functionalities. TSDSI transposed oneM2M Release 2 and submitted to DoT/ TEC for its adoption. Important points are as detailed below:

oneM2M, Release 2 specifications (transposed by TSDSI) have been adopted (14 TS out of 17, as three have become out-dated) as National Standards **(TEC 30001:2020- 30023:2020)** by TEC (details in section 9). These TEC national standards have been referred by BIS in its standard on IoT reference architecture, IoT RA IS 18004 (Part 1): 2021. TEC/ DoT referred these National standards to MoHUA and NITI Aayog for further consideration and use in Smart cities. As an extended outcome, MoHUA has referred BIS IoT Reference Architecture document in the ICCC/ ICT Model RFP 2.0 (Section-1, Volume-II: Scope of work –

Core Infrastructure) for Smart Cities and issued Advisory no. 19. (*https://smartnet.niua.org/content/6e40dcd8-ea0b-452b-b8da-c108e2f0c81f).*

8. TEC/ DoT referred U4SSC (United for sustainable smart cities) KPIs (Key performance indicators) for Smart Cities to MoHUA and NITI Aayog for further consideration and use in Smart cities.
   NITI Aayog mapped the existing KPIs of MoHUA with U4SSC KPIs and proposed creation of two new categories namely **Quality of Life: ICT Infrastructure** and **Service: Disaster Management**.

9. **IPv6 or dual stack (IPv4 and IPv6) for all the Devices / Gateways having direct connectivity with PSTN / PLMN**
   As IPv4 addresses are going to exhaust, it will be better to migrate to IPv6 as an earliest.
   - BIS in its standard IS 16444 has mandated IPv6 for Smart meters to be connected on Cellular technologies.
   - DoT has issued guidelines on IPv6 time to time[16].

10. **Licensing/ Registration for non-cellular LPWAN technologies such as LoRa, Sigfox etc. for providing communication services in IoT domain**

    Based on the recommendation in technical report on ***Communication Technologies in M2M/ IoT domain*** released in 2017, it was proposed to include non-cellular service providers in licensing / registration regime of DoT. It is important from the policy as well as security perspective to have the details of agencies providing public services. **This has been covered in UL (VNO) license released by AS cell on 17th Jan 2022.**

11. Sensors are at the bottom of pyramid for IoT systems, however, at present most of the typically used sensors are imported. Further, there is a dire need to develop new sensors all the time. Looking at these requirements, sensors need to be developed indigenously with focus on low cost, high throughput and scalable manufacturing techniques such as printing based techniques.

12. **Testing and Certification of M2M devices: -** Now it is the part of Mandatory Testing and Certification of Telecom equipment (MTCTE) regime of TEC. Essential Requirements (ERs) for the IoT devices namely Smart security camera / CCTV camera, Smart electricity meter, Smart watch, Tracking device, Feedback device, Gateways and their variants have already been finalized and uploaded on the MTCTE

[16] https://dot.gov.in/ipv6-transition

portal[17].

13. Based on TEC report on ***Code of practice for Securing Consumer IoT***, it is proposed that at least the first three guidelines as listed below should be adopted on priority: **(a). No universal default passwords ie Ban default password. (b). Implement a means to manage reports of vulnerabilities. (c). Keep software updated. (Details in section 7.5).**

14. If any IoT device is hacked or exposed to any vulnerability, it should be detected by the platform and further reported for addressing the vulnerabilities by manufacturers/ researchers. For this, a central entity like **National Trust Center** having connectivity with IoT/ Smart city platforms on open API, is required to be created for reporting of vulnerability to NTC. Details in section 7.2.

15. **Spectrum requirements for Private networks in India, based on TEC TR on Emerging Communication Technologies and use cases in IoT domain**

    1. Spectrum bands widely adopted for the industry applications are required to be considered. 3GPP TS 36.101-1 and 38.101-1 provides supported channel bandwidths in Sub-6GHz (e.g., 5, 10, 20, 40, 100 MHz) and mmWave (e.g., 200-400 MHz).

    2. Frequency bands identified for IMT globally / regionally, but not identified in India should also be considered for private networks.

    3. Frequency bands identified for IMT by India, but not assigned due to other users in limited regions (e.g., certain limited locations in the country) should be considered. A technical feasibility study/mechanism to protect incumbent users may be considered on a case-by-case basis.

    4. Contiguous spectrum is essential for providing efficient network deployment which ensures interference management. This also helps in efficient coordination for:
        - Re-use of the spectrum across multiple private industries.
        - Interference management and coordination between Public network and Private networks.

    5. Sharing / leasing spectrum from public networks may be studied/ considered.

16. **Spectrum requirement for Wi-Fi 6E technology in India – recommendation of TEC TR on Emerging Communication technologies.**

[17] https://tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments-mtcte

Study of 6 GHz band for delicensing is required, as it will be used in Wi-Fi 6E technology.

17. Close coordination among various regulatory bodies, which are related with deployment of 5G private networks / ITS applications, is essential to ensure timely and effective deployment of services for consumers.

18. Telecommunication Infrastructure development and RoW for deployment of OFC / towers be rationalized with time bound priorities across the country.

19. Concerned ministries/ departments / agencies may adopt the global best practices for automotive connectivity to accelerate the deployment of C-V2X.

20. Coordination among various related agencies at center/state government level is required for ensuring nationwide uniform adoption of technologies and standards.

21. Under BharatNet project of Government of India, a large number of Gram Panchayats (GPs) have been connected on OFC with 100 Mbps connectivity. Some of the GPs may not be having cellular coverage. For such GPs, USOF may create a mechanism for providing infrastructure such as tower, battery sets, DG set / solar panel etc. through a Telecom Service Provider (TSP)/ infrastructure provider, which may be shared by TSPs / LPWAN providers. It will help in extending smart services in rural areas.

22. An eco-system may be created for the research & development of sensor based connected devices (IoT devices) to harness the advantages of using IoT in agriculture, fisheries, animal husbandry, health care etc. Indigenous manufacturing of such devices will make them affordable for deployment in rural areas.

23. To enhance the productivity of farmers, information generated by variety of sensors deployed in the field may be analysed by a cloud based smart agriculture app which may include crop management through smart irrigation, smart pesticide control, proactive information sharing frameworks on crops and weather (using sensors, cameras, drones etc.). Options may be explored to share this data with Kisan Call Centre (1551 or 1800-180-1551) for the benefits of farmers.

24. Smart phones / Tablets/ Laptops may be out of the budget of the economically poor households. Low cost devices with minimum features such as Wi-Fi, Bluetooth, cellular connectivity and long battery life are required to accelerate the use of technology in various applications in rural areas.

25. Smart City platforms should be able to manage the emergency health services to the public of city as well as rural areas by analysing data from the connected health care devices as well as respond to the calls of the public, especially in a pandemic situation.
26. Technology for Smart cities– both legacy and new requirements should be standards compliant and conform for interoperability in general. Standards released by various National / International bodies such as ITU, ETSI, 3GPP, oneM2M, IEEE, NIST, BIS, TEC etc. may be followed to ensure interoperability.
27. A framework needs to be created for access to national databases like UIDAI, CCTNS, NCRB, etc. for security & surveillance systems.
28. Biometric authentication of users using Aadhaar (UID) database and UID Number may be adopted as the authentication process for electronic health record system. A design and implementation plan for this work item needs to be created.
29. Cities should use available resources - smartphone-based sensor-networks as well as crowdsourced data from its citizens to enrich its services where possible.
30. The different city services should break walls and share data. Common Service principles/Common Service layer and Open Data concepts should be adopted by Cities.
31. Smart City planners should employ Design, Systems and Future thinking frameworks to conceptualize, design and develop solutions using IoT that are long lasting and resilient.
32. Society 5.0, a super smart nation with digitalization across all levels of society, to positively transform India is what we should work towards.
33. There is a need for proper town planning using GIS for efficiently deploying various solutions such as traffic management, street light, waste management etc.

8.2. Recommendations from the report- Security by design for IoT device manufacturers, released in March 2023

8.2.1. Generic requirements for IoT device security

1. TEC TR Code of practice for securing Consumer IoT (refer section 3.2.2) may be widely circulated among the related stakeholders (IoT device manufacturers, Service providers, System Integrators, Application Developers & Researchers etc.) for adopting / following these guidelines.

2. Based on the studies mentioned in sections 3.2(TEC), 4.7(IoTSF), 4.8(NIST), 4.13.2(IMDA Singapore), 4.14(UK regulation), 4.16(US IoT Bill)and 4.18(World Economic Forum), it is proposed that at least the first three guidelines of TEC TR Code of Practice for Securing Consumer IoT as mentioned below may be adopted on priority by related stakeholders.

i. No universal default passwords.

ii. Implement a means to manage reports of vulnerabilities.

iii. Keep software updated (Provide transparency on for how long the product will receive security updates). An update should be easy to implement, preferably using non-intrusive approaches like over the air (OTA) updates. It may be treated as baseline requirement for the IoT device manufacturers and other related stakeholders. It is recommended that DoT may make above guidelines as mandatory practice in near future.

3. As mentioned in 2(ii) above, vulnerability reporting should be mandated by making it part of policy / regulatory requirement as the security of IoT products diminishes over time and the risk of attack or abuse increases (refer section 4.7.1).

4. IoT vendors (IoT device manufacturers or their authorized representatives) being an important entity of the IoT eco system, should declare Vulnerability management policy on their websites (to publish a clear and transparent vulnerability disclosure policy; establish an internal vulnerability management procedure; make contact information for vulnerability reporting publicly available; and continuously monitor and identify security vulnerabilities within their products) (refer sections 4.5, 4.14 & 4.7.4).

5. End-of-life devices or the devices not getting updates may be highly vulnerable and threat to the network. The Platforms (refer section 3.2.1) should be able to report information about such cases to NTC. Such type of devices needs to be replaced /disconnected in the time bound manner. Policy guidelines need be developed for the same.

6. Device classification as proposed in section 6.4 may be adopted for India. It is required to make consumer aware about the guidelines available in point-2 and the labelling/ classification of the devices so that the consumer may decide as per their security needs.

7. ITU-T X.509 based digital certificates may be used for secure on boarding of IoT devices and to manage the device lifecycle in public key infrastructure using digital signature and code signing./)Refer sections 1.2, 4.1 and Annexure-IV(.

8. IoT device manufacturers should test the devices against known vulnerabilities before release in the market./To begin with, critical devices and network elements such as IoT Gateway, Smart Camera, Smart Watches, Smart phones, Smart meters, tracking devices, Smart door locks, Wi-Fi routers, Optical Network Terminal)ONT(, Broadband modem, switches, routers etc. may be tested./This requirement may be included in the ITSAR of related devices.

9. It is proposed that the first three guidelines as mentioned in point no./2 above may be included in security specification (ITSAR) of IoT devices being prepared by NCCS, Bangalore. To begin with, the/devices/mentioned/in/point/no./8 may/be/taken.

10. All IoT devices except those falling in Leve-0 of classification scheme should have a secure boot mechanism. (refer sections 1.2.1 and 6.4)

11. Firmware/ Operating System/ Applications needs to be updated through secure mechanism. (Refer Section 1.2)

12. Devices to be used in critical installations/ public networks should have a forced mechanism for changing the factory password by the user prior to its first use.

13. Platform providers are also the M2M/ IoT Service providers. Generally, the M2M/ IoT Service providers empanel the device manufacturers. All the M2M/ IoT Service providers should register with DoT.

14. Regular monitoring of network traffic at the gateway or platform may help in early detection and prevention of potential security threats.

8.2.2. Hardware security recommendations

1. Supply Chain Security is required for components used in product development process. Active programming code that resides in supply chain components should be subjected to security /quality check process (refer section 2.3).

2. IoT devices should have standard encryption methods./Lack of encryption is a threat to the device and its reliability./Encryption of data at rest and at motion is vital./Any information that is not encrypted with the right set of protocols can be collected by attackers and used to forcefully access the enterprise environment (refer section 5).

3. Hardening of end point devices working in the network is essential.

4. Root of Trust technology may be enabled in IoT device to strengthen the security (refer sections 1.2, 4.9.1, 7.2).

5. For SIM based devices following hardware security provisions are recommended: i. UICC/eUICC enabled IoT device shall reserve minimum 32K of Non-Volatile Memory (NVM) space for installing Government notified application like disaster management, social welfare, security, health, safety. (Ref:/ UICC ITSAR http://nccs.gov.in). ii. To protect SIM from IMSI catcher, Subscription Concealed Identifier (SUCI) and Subscription Permanent Identifier (SUPI) should be integrated in SIM for 5G cellular technology security. iii. For eSIM business in India, the certificate issuer for eSIM Remote Service Provisioning (RSP) needs to be located in India under GSMA. iv. In view of security of IT infrastructure related to eSIM remote service provisioning (SM-DP, SM-SR and SM-DP+), these IT infrastructures need to be owned by any registered entity with DoT and located within Indian territory.

6. Firewalls and access controls may be implemented to restrict unauthorized access to IoT devices and networks.

7. To address the possible threat due to emerging Quantum computing, it is important to study how Quantum Key Distribution (QKD0 can be used to secure an IoT system. QKD is a viable solution to counter the threats that may appear in future from quantum computers thereby securing all IoT related applications (refer section 4.6.4.).

8.2.3. Software security recommendations

1. IoT devices are recommended to support the possibility to verify software image integrity at boot time (refer section 4.7.5).

2. IoT devices' operating system (OS) development, its functional testing, validation and security implementation along with its security testing are required to be done in a secured and certified protected environment (refer section 3.5.1 - NPE 2019 and TEC National Trust Centre Report).

3. All keys, certificates, or the credentials should be changeable and stored securely in the IoT device.

4. Implementation of cryptography functions are required to resist the side channel attack such as cache memory timing attack, power and electromagnetic (EM) analysis attack (refer section 1.1).

5. The operating systems should have mechanisms to authenticate applications while they are in an active or dormant state and have access to sensor data.

6. Software update integrity may be verified using the secure cryptography controls.

7. For critical and sensitive use cases, it is required that IoT devices enabled with Trusted Execution Environment (TEE) ensure data protection even if the device operating system is compromised (refer section 5).

8.2.4. Policy related recommendations

1. TSPs should provide the telecom resources only to the registered M2M/ IoT Service providers with DoT.

2. Related Standard Operating Procedure (SoP) and ITSARs should be implemented and regular audit mechanism should be in place.

3. For promoting IoT security, domestic IoT device manufacturers and other stakeholders, as applicable, may be incentivized for a limited period for adopting the IoT security baseline requirements.

4. IT infrastructure of OEM initiating the Software update (Patch loading) should be registered and operated from Indian Territory.

5. The recommendations available in section-4 (Policy intervention required for the development of NTC) of the TEC TR Framework of National Trust Centre for M2M/IoT Devices and Applications need to be implemented on priority.

9. Adoption of TSDSI / International Standards

Telecommunication Engineering Center (TEC) is the National Standardisation Body for Telecom and related ICT sector in India. "**Standardization Guide –A policy document for adoption of Domestic/ international standards into national standards**[18]" was issued vide O.M. No. 2-1/2018/SD/TSDSI/TEC/5 dated 08-05-2020.

TSDSI (Telecommunications Standards Development Society of India) is a membership based, standards development organization(SDO) for Telecom/ICT products and services in India. TSDSI is a Partner Type I member of oneM2M and 3GPP.

TSDSI transposed oneM2M Release 2 specifications, submitted by TSDSI to DoT, were forwarded to TEC in Jan 2018, for considering them for adoption / ratification.

[18] https://tec.gov.in/standards-adoption-policy

TEC, after complying with the consultation process as per the Standardisation guide, adopted oneM2M Release 2 specifications (14 TS out of 17, 3 TS dropped being outdated) as National standards, which are available on TEC website[19] as TEC 30001:2020- 30023:2020. These national standards shall be voluntary unless made mandatory by its use, reference or adoption by regulation / Govt. directive.

Later on in August 2022, TEC adopted oneM2M Release 3 specifications (24 TS) as National Standards and the same was notified via O.M. No. 19-01/2020-STD/TEC, dated 01-08-2022. These standards are available on TEC webpage[20] as TEC 30001:2022- 30035:2022.

10. International Recognition of TEC Technical Reports

1. International Telecommunication Union (ITU) has posted the following six TEC Technical Reports on its website (https://www.itu.int/cities/dt-resource-hub/iot/) in IoT sections (2023, 2022 and 2021), recognizing them as insightful technical resource for the benefit of global community-

   i. Security by design for IoT Device Manufacturers
   ii. Framework of National Trust Centre for M2M/IoT Devices and Applications
   iii. IoT/ ICT Standards for Smart Cities
   iv. Emerging Communication Technologies & Use Cases in IoT Domain
   v. Code of Practice for Securing Consumer Internet of Things (IoT)
   vi. IoT/ ICT Enablement in Smart Village and Agriculture

2. TEC Technical report ***Code of practice for securing consumer IoT*** has been mentioned by several international organizations such as IoTSF.

11. Contributions at International level on IoT & Smart cities

1. IoT division TEC submitted contributions in almost all the meetings of ITU-T SG-20 and presented physically / virtually. Important achievements are:

   a. Work item Y. SRC on ***IoT and ICT Requirements for deployment of smart services in rural communities*** approved as ITU-T standard in ITU-T SG-20 meeting, Jan-Feb 2023 and is under publication as ITU-T Recommendation Y.4218 (05/2023).
   Mr. Sushil Kumar, DDG (IoT) and Ms. Namrata Singh, ADG (IoT) have worked as editors in this work item.

[19] https://tec.gov.in/onem2m
[20] https://tec.gov.in/pdf/M2M/M2M_TR_TS-Rel-3.pdf

b. **ITU-T Recommendation Y Suppl. 53 (12/2018)**[21] on **IoT use cases** having following IoT use cases [first five (1 to 5) submitted from TEC, India and one (at s.no. 6) from Egypt] :

1. Vehicle emergency call system for automotive road safety
2. Digitization and automation of Vehicle Tracking, Safety, Conformance, Registration and Transfer via the application of e-SIM and Digital Identity
3. Remote monitoring the health of a patient
4. Connected Smart homes.
5. AMI (Advanced metering infrastructure)
6. RFID Based Digital Identification for Vehicle Tracking, Registration, and Data Transfer.

c. **ITU-T Recommendation Y Suppl. 56 (12/2019)**[22] on Smart city use cases, having smart city use cases from Japan, Korea, UK and India. Use case submitted by TEC is as given below:

- Intelligent Traffic Management System, Adaptive Traffic Control System, CCTV based Real Time Public Safety System, Solid waste management and Integrated platform with command & control center (ICCC) for a Smart city.

These use cases (at point no. 'b' and 'c') may be implemented to create smart infrastructure, which will resolve a number of issues of the respective vertical and in turn improve the quality of life.

Sushil Kumar, DDG(IoT) worked as an editor in both the standards mentioned above at 'b' and 'c'.

Mr. Marco Carugi, ITU-T SG-20 Q2/20 Rapporteur and Dr. Chaesub Lee, ITU-T TSB Director appreciated the efforts and dedication of Indian team.

d. Following three contributions submitted by IoT division TEC have been approved in **ITU/ FAO Focus Group on 'Artificial Intelligence (AI) and Internet of Things (IoT) for Digital Agriculture' (FG-AI4A)** meetings in 2022-23-

i. *Applications of Drones, AI and IoT in Cashewnuts farming (based on the project in VIT Chennai)*
ii. *IoT based Farmland Surveillance System with Disease Detection in Paddy Crops (based on the project in VIT Chennai)*
iii. *Artificial Intelligence-based Disease Identification in Wheat Crops (based on the project in ICAR, New Delhi)*

These were presented jointly by TEC officers and the members from VIT/ ICAR.

[21] https://www.itu.int/itu-t/recommendations/rec.aspx?id=13867&lang=en
[22] https://www.itu.int/itu-t/recommendations/rec.aspx?id=14174&lang=en

e. IoT division submitted contribution on ***IMT applications in utilities*** for Draft Report ITU-R M. [IMT.INDUSTRY] for ITU-R WP 5D (#42) meeting, 10-21 October 2022. Same was presented virtually.

f. IoT division submitted a contribution in ITU-T SG-17 meeting, Feb 2023 as ***Revision of TD616 X.sc-iot: Security Controls for Internet of Things (IoT) systems***. Same was presented virtually and included in the draft document with some minor changes.

2. Contributions in APT meetings:

a) Contributions were submitted and presented in APT WTSA-20 meetings, 2020 on ***Resolution 98 "Enhancing the standardization of Internet of things and smart cities and communities for global development"*.**

It has also been discussed and finalized in WTSA meeting, Geneva, March 2022.

b) Following contributions were prepared, submitted and presented on behalf of Indian Administration in **26th Meeting of APT Wireless Group (**AWG-26 Meeting), September 2020.

i. Proposal for working document towards a draft new APT Report on "***Technology and Spectrum Management Techniques for IoT Networks***"

ii. Proposal for LTE and 5G NR based V2X in Working Document Towards "***Cellular Based V2X for ITS applications in APT Countries***"

These contributions have been incorporated suitably in the documents under development.

12. IoT Experience Center in TEC

IoT Experience Center in TEC was established in 2019. It is having 17 use cases working in real time on various communication technologies. Some of them are as given below:

1. Vehicle tracking device having Embedded SIM and working on cellular technology from 2 or more Telecom Service Providers as mandated by MoRTH in AIS140.

2. Feedback devices working on Cellular / LoRa technologies.

3. IoT Gateway having interfaces for various communication technologies like 6LowPAN, NFC etc. in LAN and Cellular (2G/ 3G) in WAN.

4. Smart lighting systems for homes/ buildings/ hotels working on Bluetooth / Bluetooth Mesh and can be controlled Smart phone.

5. Smart Street lighting solution working on LoRa communication technology.

6. Smart home – Door sensor with camera working on Z-wave, Wi-Fi and cellular technology.

7. Temperature/ humidity measuring devices, woman safety device on LoRa communication technology.

8. Parking sensor on LoRa communication technology.

9. Prototypes on LoRA and LTE

These use cases have been provided by TEC - IoT Working Group members.

13. PM Gati Shakti event

TEC organised a panel discussion on M2M/ IoT & 5G enabling Smart infrastructure in PM Gati Shakti event held on 13th Oct. 2021. This panel was moderated by Sr. DDG TEC and having DDG(IoT) TEC, JS – Smart City mission MoHUA and industry experts from Sensorise, STMicroelectronics and AAEM Test lab as panel members. Following recommendations are the outcome of the panel discussion:

1. Creation of National Trust Centre (NTC) for security systems. Incentivize stakeholders' compliance and research to address threats and vulnerabilities.
2. Incentivize M2M/ IoT device manufacturing, R&D and providing solutions in different verticals like Advanced Metering Infrastructure (AMI), Automotive, Health care, Telematics, Road safety, Smart Cities etc.]
3. Enable conducting pilots/Proof of Concept to give opportunities to local entrepreneurs
4. Enable Indian MSMEs participation in International standardization
5. MSME and Mid-market companies should have easy and frugal access to test and certification infrastructure,
6. All the Certification required for Indian IoT services must be locally handled by TEC accredited labs in India, including international certifications such as GSMA SAS, oneM2M, ETSI, CTIA etc.
7. M2M Service Provider Registration policy and process are critical and a pre-requisite for security initiatives of the government

8. Harmonization of Standards: One testing One Certificate which is acceptable globally
9. Policies for incentivising the Creation, Registration, Protection, Recognition, Promotion, Monetization of Indian IPR
10. Dramatic improvements in the accountability and responsiveness of the Indian Patent Office
11. Dedicated program may be introduced in universities to address the shortage of skilled manpower
12. Exploring U4SSC - ITU KPIs for smart cities in Indian environment
13. Taxes on capital equipment and lab setups can be relaxed
14. Emergence of common platforms in line with Gati Shakti to increase use cases for IoT devices and the need for standardization
15. Incentivized Spectrum for C-V2X, Low Power Wireless Communication Technologies and private industrial networks
16. DoT-NITI Aayog – MoRTH coordination for Intelligent Transport Systems

14. Important work items in progress in IoT division, TEC

a. EMF exposure from IoT devices
b. Emerging Technologies and standards for Intelligent Transport System
c. IoT and 5G Use cases in Agriculture
d. IoT and 5G applications in Smart Grid
e. Preparation of Essential Requirements under MTCTE regime
f. Technical evaluation of applications for Conformity Assessment Bodies (CABs)/ Certification Bodies (CBs) for performing testing and certification of telecom products under MTCTE regime.
g. Participation and submitting contributions in ITU-T SG-20 and other national / international meetings.
h. Arranging webinars/ workshops/ conferences related to IoT and Smart cities

15. Participation/ positions at national/ international level

15.1. Participation

1. Officers of IoT division are the members in various NWGs in TEC and LITD committees of BIS (LITD-27 and LITD-28).

2. In addition to the participation in ITU, ISO IEC JTC1 SC41 meetings/ webinars, there is regular participation by the officers of IoT division in NIST, ETSI

Security week, ETSI IoT week, oneM2M and also in other national/ international virtual meetings / webinars.

3. DDG (IoT) participated in around 175 National / international Conferences/ webinars/ faculty development programmes/ training programme as a speaker/ moderator/ chair on IoT, Smart City, 5G and digital transformation related topics.

15.2. Positions

1. Mr. Sushil Kumar, DDG (IoT) holds following positions at international and national level:-

i. Chairman- **ITU-T SG-20 Regional Group for Asia Pacific region**
ii. Vice-chair - **ITU-T SG-20 WP2/20**
iii. Vice-chair- **ITU/ FAO Focus Group** on ***'Artificial Intelligence (AI) and Internet of Things (IoT) for Digital Agriculture (FG-AI4A)'***
iv. Vice-chair- **APT Preparatory Group for WTSA-24**
v. Expert member- **IEC- ISO- ITU Joint Smart City task force (J-SCTF)**
vi. Member - Advisory group of ISO/ IEC JTC1 SC41
vii. Chairman- **National Working Group (NWG-20)** of TEC for preparing and submission of contributions to ITU-T SG-20 on Internet of things (IoT) and smart cities and communities (SC&C)
viii. Chairman- **BIS national committee (LITD- 27)** on *IoT and Digital Twin* to coordinate with ISO/ IEC JTC1/ SC 41 and participates as a head of Indian delegation in ISO/ IEC JTC1/ SC 41 meetings

2. Ms. Namrata Singh, ADG (IoT) holds following positions at international and national level:-

i. Vice-chair- Working Group for *Mapping and Analyzing AI and IoT standards related Activities in Digital Agriculture* under Focus Group on *'Artificial Intelligence (AI) and Internet of Things (IoT) for Digital Agriculture (**FG-AI4A**)'*
ii. Convener- **National Working Group (NWG-20)** of TEC

3. Dr. Bala Murugan MS, professor from VIT Chennai is the Chair of Working Group on *Glossary (WG-Gloss)* under FG-AI4A.

4. Dr. Vydeki D, professor from VIT Chennai is the Vice-chair of Working Group on *Digital Agriculture Use Cases and Solutions (WG-AS)* under FG-AI4A.

Annexure- Communication technologies and related IoT applications

Technology/ Protocol	Frequency band (s)	Technological advantages	Technological limitations	Suitable for
1. Low power short range technologies				
Bluetooth Low Energy	2.4 GHz	• Mature technology • Easy to implement • Low Power • Powered by coin cell • Longer battery life	• Small data packets	• Healthcare devices • Fitness devices • Remote Health Monitoring • Smart Metering
NFC	13.56 MHz	• Consumes less power • Almost instantaneous connectivity between devices • No power is required in-case of passive Tags	• Extremely short range • Expensive • Low information security • Low market penetration	• Healthcare devices • Fitness devices • Smart Metering
Wi-Fi 4 IEEE 802.11n Wi-Fi 5 802.11ac	2.4 GHz and 5 GHz 5 GHz	• Mature technology • High home/office penetration • High data rates achievable • Easy to implement Wi-Fi 4 uses MIMO while Wi-Fi 5 MU-MIMO technology Max throughput speed Wi-Fi 4 : 600Mbps Wi-Fi 5: 3.5 Gbps	• Limited range • Poor building penetration • High interference from other sources • Power consumption higher than those technologies that operate in the sub-GHz band	• Base station in Health Clinics • Smart Metering • Home Automation
Wi-Fi 6 IEEE 802.11 ax	2.4 GHz and 5 GHz	• MU-MIMO and OFDMA technology • Max throughput speed 9.6 Gbps		• For better user experience even for dense indoor/outdoor deployments such as airports, railway stations, shopping malls, stadiums, homes, school campuses
Wi-Fi 6 E IEEE 802.11 ax devices capable of operating at 6GHz also.	2.4 GHz, 5 GHz and 6 GHz	• 6 GHz band provides 1200 MHz additional spectrum to Wi-Fi 6 enabled devices, Which Doubles the bandwidth and throughput of Wi-Fi 6 enabled devices.	• Smaller range compared to 5GHz spectrum • 6 GHz band (5.925 GHz to 7.125 GHz) is required to be delicensed.	• Applications like 8K video, AR/VR gaming and mission critical requirements.
Wi-Fi HaLow IEEE 802.11 ah	900 MHz delicensed band	• Low power • Longer connectivity range (approx. 1 Km)	• Comparatively larger antenna size	• IoT use cases in industrial applications,

		• IP support available		agriculture, health care smart building, smart homes and smart city
Z-Wave	Sub 1GHz (865-867 MHz) for India	• Standardised by CSR 564 (E) • very successful due • to its ease of use and interoperability • Majority share of the Home Automation market	• Proprietary radio systems available • Limited Range drives up costs	• Security systems. • Home automation. • Lighting controls
2. Cellular technologies				
Cellular (2G-GSM/EDGE, 3G-UMTS, 4G-LTE)	Country or region specific	• Mature technology • Developed by global community of 400+ companies from 39 countries • Rapid deployment • Communication modules are low cost and standardised. • Roaming • Wide availability of Network Infrastructure	• Coverage not 100% • Reliability not the best • Short technology life-cycle (2G, EDGE, 3G, LTE etc.)	• Tele-Health • Remote Health Monitoring • Smart Metering • Remotely switching ON/ OFF the water pump in rural areas,using mobile phone
Cellular 5G: (Radio Interface technology approved by ITU)	Country or region specific	• High speed internet services (eMBB) • Low latency (<1ms) (uRLLC) • Large number of devices may be connected / Sq Km. (massive M2M) • Wider coverage • Technology for vertical applications		• e-Governance • Remote surgery • Drones, • Remote maintenance of machines • Precision agriculture • Livestock monitoring and management
3. Cellular low power wide area network technologies				
Cellular: EC GSM IoT	Country or region specific	• Network infrastructure is backwards-compatible to previous releases to allow the technology to be introduced into existing GSM networks	• Eco system is yet to be developed	• Smart cities & homes • Smart utilities • Industrial automation • Wearables • Smart energy • Intelligent transport systems
Cellular: NB-IoT	Country or region specific	• Standards based defined by 3GPP, the global standardization organizations supported by a	• Limited Mobility is not yet supported (limited support based on cell reselection)	• Sensor based applications, with low data rate requirement. • Applications not

		mature global ecosystem • wide area ubiquitous coverage • deployed through upgrade of existing network (reuses existing network infrastructure) • Ultra-low-power consumption in devices • Enhanced for 20+dB additional coupling gain. (reaches deeper in-building & underground) • low cost terminal • plug and play • high reliability and high carrier-class e2e network security (based on LTE)	• Voice is not supported • Low Data rate applications with link peak DL = 60~100kbps & UL=~50kbps	requiring high speed mobility handovers. • Systems where devices/sensor measurements are expected to be for long ~10years
Cellular: eMTC	Country or region specific	• Developed by 3GPP a mature global ecosystem • Low power consumption • Works over existing LTE networks • Easily configurable on demand scaling possible • Supports full mobility • Supports voice through VoLTE • high reliability and high carrier-class e2e network security (based on LTE)	• Support of higher bandwidth limits the other optimizations possible, compared to NB-IoT and EC-GSM-IoT	• Wearables, • Asset Tracking, • Pet Trackers • Telematics, • KIOSK, • Parking, • Industry environment monitoring, • Connected Healthcare personal & Enterprise equipment • Industrial IoT with Emergency Voice call support
4. Non cellular low power wide area network technologies				
LoRaWAN (https://lora-alliance.org/)	Sub 1 GHz (865-867 MHz) for India	• Network can be defined by the individuals / owners. • Support long range and high battery life • High security using AES 128 encryption • Low cost infrastructure	• Own deployment with no subscription fees • Works in unlicensed band. • Limited data rate and payload size	• Smart Metering, • Smart street Lighting solutions • Asset monitoring • Tracking • Transmission of soil data, transmitting fire alerts etc. • Weather forecasting • Environment

				(Co2,CO,humidity, Temperature etc) Monitoring
5. Wireline technologies				
DSL		• Inexpensive (installation and use) • High SLA • Less installation time • Bonded DSL provides inherent redundancy	• Low data security • Lower throughput • Higher latency	• Gateway for Remote Health Monitoring • Concentrator for Tele-Health • Home Automation
Ethernet		• Inexpensive (installation and use) • Excellent throughput • Low installation time • Easily scalable	• Lowest data security • Lowest SLA • Highest latency • Bursts of additional bandwidth not possible	• Gateway for Remote Health Monitoring • Concentrator for Tele-Health • Smart Metering • Home Automation

Compiled by following officers:

Name	Designation	Organization	E-mail address
Sushil Kumar	DDG (IoT)	TEC	ddgsd.tec@gov.in, sushil.kumar20@gov.in
Ms. Ashima	Dir (IoT)	TEC	dirsd1.tec@gov.in
Ms. Namrata Singh	ADG (IoT)	TEC	namrata.singh51@gov.in
Shekhar Singh	AD (IoT)	TEC	ad.iot-tec@gov.in

ISO 9001:2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA