



TECHNICAL REPORT

Security by Design *for* IoT Device Manufacturers

TEC 31328:2023

Security by Design and National Trust Centre Working Group



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

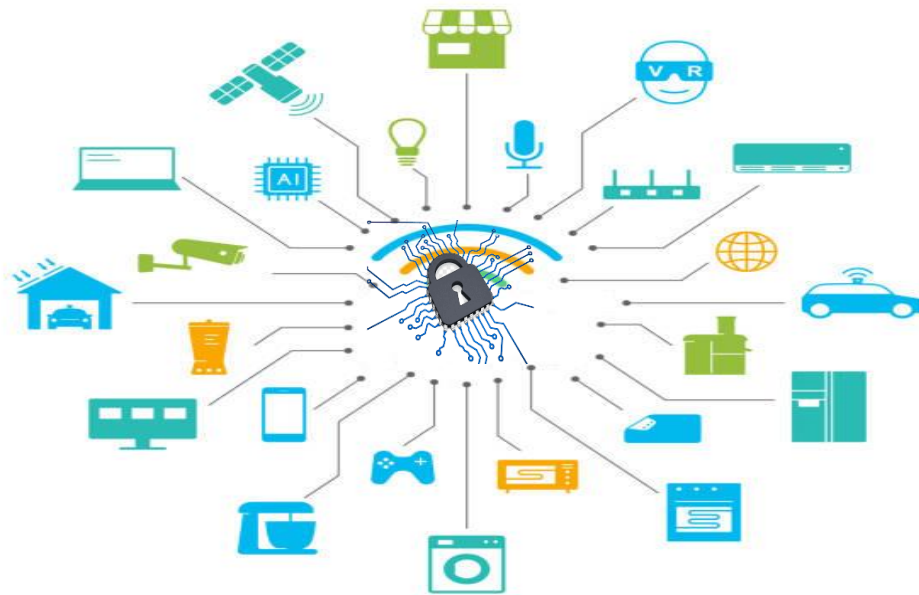


TECHNICAL REPORT

Security by Design *for* IoT Device Manufacturers

TEC 31328:2023

Security by Design and National Trust Centre Working Group



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

Revision History

Date	Release	Document No.	Description
August, 2021	R1.0	TEC 31318:2021	Code of Practice for Securing Consumer IoT
31-03-2023	R2.0	TEC 31328: 2023	Security by design for IoT Device Manufacturers

Important Notice

Individual copies of the present document can be downloaded from <http://www.tec.gov.in>

Users of the present document should be aware that the document may be subject to revision or change of status.

Any comment/suggestions may please be sent to:m2mreports.tec@gov.in

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.

के. राजारामन, भा. प्र. से.
सचिव
K. Rajaraman, IAS
Secretary



सत्यमेव जयते



भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
Government of India
Ministry of Communications
Department of Telecommunications



Message

I am pleased to share that Telecommunication Engineering Centre(TEC) has prepared a Technical Report on **Security by Design for IoT Device Manufacturers**, which is intended to serve as a guiding document for the IoT device manufacturers and other related stakeholders.

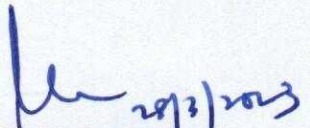
TEC has previously released eighteen Technical Reports covering various verticals of IOT domain, viz., Automatic, Power, Health, Safety & Surveillance, Smart Homes, Smart Cities and the horizontal layer – M2M Gateway & Architecture, Communication Technologies and IoT Security. ITU has posted five TEC Technical Reports in IoT domain on its global portal recognizing as an insightful resource for the member states. Report on *Code of Practice for Securing consumer IoT* has been mentioned in several international documents.

The rapid growth of the Internet of Things (IoT) has led to an explosion of connected devices, providing unprecedented levels of convenience and functionality. However, this increased connectivity has also led to significant security concerns. As more and more devices become connected to the internet, the attack surface for potential threats becomes larger, making IoT security a critical issue.

This report includes study of threats, challenges and national as well as international standards, best practices and guidelines to mitigate these challenges related to IoT device security. This report also provides the detailed recommendations for the IoT device manufacturers and other related stakeholders.

I hope that this technical report will be helpful in securing the IoT ecosystem in the country. I appreciate the sincere efforts put in by Telecommunication Engineering Centre in bringing out this report. I wish them success in all their future endeavors.

Date: 28.3.2023
Place: New Delhi


(K Rajaraman)

उमा शंकर पांडेय, भा.दू.से.
सदस्य (सेवाएं)
Uma Shanker Pandey, ITS
Member (Services) &
Ex-officio Secretary to Govt. of India



75
आज़ादी का
अमृत महोत्सव

भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग, डिजिटल संचार आयोग
संचार भवन, 20, अशोक रोड, नई दिल्ली-110001
Government of India
Ministry of Communications
Department of Telecommunications
Digital Communications Commission
Sanchar Bhawan, 20, Ashoka Road,
New Delhi - 110001
Ph. : 011-23714644, Fax : 011-23755172
E-mail. : members-dot@nic.in

Message

I am delighted to announce that the Telecommunication Engineering Centre (TEC) is bringing out a Technical Report on **Security by Design for IoT Device Manufacturers**.

It is appreciable that TEC has released eighteen Technical Reports in the last 4-6 years covering various verticals, communication technologies and Security in M2M/ IoT domain. Important actionable points emerged from these reports are being used in the development of standards / policies; enabling the proliferation of IoT ecosystem in the country.


Security of the IoT domain, from devices to the applications becomes a matter of paramount importance as hacking of the devices / network being used in daily life will harm companies, organisations, nations and more importantly people. It may result in collapse of the services, creating panic and may result in chaos.

I am delighted to share that this technical report has elaborated the standards and best practices related to IoT device security based on National / International standards, guidelines & best practices.

This report has also covered the standards released by ITU-T SG-17 & SG-20, ISO/IEC JTC-1 SC27, NIST, ETSI, ENISA, CSA Singapore etc. and the best practices from UK-DCMS, IoTSF, World Economic Forum (WEF) etc.

I hope this document will be a good resource as the recommendations available in this report may be quite useful for the IoT device manufacturers and other related stakeholders.

I appreciate the efforts put in by IoT division, TEC and I congratulate them for all their hard work and best wishes for the future.


(Uma Shankar Pandey)

New Delhi
Dated: 28.03.2023

2/3

संजीव अग्रवाल
सदस्य (प्रौद्योगिकी)
Sanjeev Agrawal
Member (Technology)



भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग, डिजिटल संचार आयोग
संचार भवन, 20, अशोक रोड़, नई दिल्ली-110001
Government of India
Ministry of Communications
Department of Telecommunications
Digital Communications Commission
Sanchar Bhawan, 20, Ashoka Road,
New Delhi - 110 001
Ph. : 23372307, Fax : 23372353
E-mail : membert-dot@nic.in

Message

I am pleased to note that Telecommunication Engineering Centre (TEC) is bringing out a Technical Report on *Security by Design for IoT Device Manufacturers*. This report is in continuation to the series of eighteen technical reports already released having three reports related to IOT security.

DoT has endorsed the report Code of Practice for securing consumer IoT to the ministries, TSPs and M2M SPs as an advisory to follow at least the first three guidelines namely No universal default passwords, implement a means to manage reports of vulnerabilities and keep software updated as it will help in securing consumer IoT ecosystem.

IoT technology is being used across the globe to create Smart infrastructure in various sectors namely energy, transportation, banking, critical services, water management, smart homes, Smart cities etc. These smart infrastructures are subjected to vulnerability and cyber-attack. Therefore, the security of the end points and connected elements is of prime importance.

TEC has also adopted one M2M Release 2 and Release 3 specifications as National Standards. It is an important step towards developing standards based IoT ecosystem. TEC has also developed specifications on IoT security.

This technical report covers the standards the standards, best practices and guidelines related to IoT device security based on National/ International study.

I hope this document will be a useful resource for all the related stakeholders. I appreciate the efforts of Telecommunication Engineering Centre specially its IoT Division and the members of the Working Group for bringing out this technical report in a very timely manner. I wish them success in all their endeavors.

Date: 28.03.2023
Place: New Delhi


(Sanjeev Agrawal)

ऋतु रंजन मित्र

RITU RANJAN MITTAR

वरिष्ठ उप महानिदेशक एवं प्रमुख

Sr. Deputy Director General & Head



सत्यमेव जयते

भारत सरकार

दूरसंचार विभाग

दूरसंचार अभियांत्रिकी केन्द्र

खुर्शीद लाल भवन, जनपथ, नई दिल्ली-110001

Government of India

Department of Telecommunications

Telecom Engineering Centre

Khurshid Lal Bhawan, Janpath, New Delhi-110001

Foreword

TEC is the National Standardization Body (NSB) for telecommunication in India and the national enquiry point for WTO-TBT (Technical Barrier to Trade) for telecom sector. TEC has also been mandated to interact with various international standardization bodies like ITU, APT, ETSI, IEEE, oneM2M, 3GPP etc. for standardization works.

TEC takes up development of standards based on study, continuous participation/submitting contributions in the meetings of standardization bodies and interaction with stakeholders.

M2M/ IoT is one of the most emerging technologies and it is being used to create smart infrastructure in various vertical industries and also in Smart cities. As per NDCP 2018, developing framework for accelerated deployment of M2M services while safeguarding security and interception for M2M devices has to be ensured.

TEC has already released eighteen Technical Reports covering various verticals viz. Automotive, Power, Health, Safety & Surveillance, Smart Homes, Smart Cities, Smart Village & Agriculture and also in horizontal layer, the documents namely V2V/V2I Radio communication & Embedded SIM, Communication Technologies in M2M/ IoT domain, M2M Gateway & Architecture, M2M/ IoT security etc. All the technical reports are available on TEC website (<https://tec.gov.in/M2M-IoT-technical-reports>). Important actionable points emerged from these reports are being used in the development of standards / policies; enabling the proliferation of IoT ecosystem in the country.

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

1. Framework of National Trust Centre for M2M/IoT Devices and Applications,
2. IoT/ ICT Standards for Smart Cities
3. Code of practice for Securing Consumer IoT
4. Emerging Communication Technologies & Use Cases in IoT Domain
5. IoT/ICT Enablement in Smart Village and Agriculture

Guidelines available in ***Code of Practice for Securing Consumer IoT*** may provide a direction to the related stakeholders in provisioning of secured consumer IoT devices and also help in reducing the vulnerabilities.

DoT has issued the Office Memorandum (OM) 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 and provide feedback. Recently, DoT has also issued an advisory to M2M service providers for following first three guidelines available in this report.

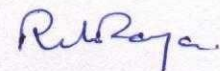
TEC has adopted oneM2M Release 2 as well as Release 3 standards (transposed by TSDSI) as National standards (<https://tec.gov.in/onem2m>). It is also the having specifications related to IoT security in TS-0003.

The TEC Working group on *Security by Design Principles for IoT Device Manufacturers and NTC* is having members from Government, industry, academia, R&D organisations and start-ups. Around 45 virtual meetings and a number of short meetings/ discussions have already been held in drafting and finalizing the content of the Technical Report titled ***Security by Design for IoT Device Manufacturers***. As a part of this working group two technical reports namely *Code of practice for Securing Consumer IoT* and *Framework of National Trust Centre for M2M/IoT Devices and Applications* have already been released.

This report covers the recommendations related to IoT device security based on National / International standards, guidelines & best practices including standards released by BIS, ITU-T SG-17 & SG-20, ISO/IEC JTC-1 SC27, NIST, ETSI, ENISA, CSA Singapore etc. and the best practices from UK-DCMS, IoTSF, World Economic Forum (WEF), STQC etc.

This report is expected to provide guidance to all concerned stakeholders.

I appreciate the efforts put in by officers of IoT division and working group members in bringing out this report. I wish them success in all their future endeavors.



(R. R. Mittar)

Table of Contents

List of Contributors	iii
Executive Summary.....	1
1. Introduction to M2M/ IoT	4
1.1. IoT Device	5
1.2. IoT Product requirements and developer’s initiative	6
1.2.1. Identity management for M2M/IoT devices.....	8
1.3. IoT Device – Security Challenges.....	10
2. Attacks, Vulnerabilities, Threats in IoT domain and Risk mitigation.....	11
2.1. Cyberattacks.....	11
2.2. IoT - Threats & Vulnerabilities	15
2.3. Risk Mitigation Areas.....	21
3. Existing policies, standards and guidelines related to M2M / IoT security.....	24
3.1. DoT policies in M2M/ IoT domain	24
3.1.1. National Digital Communication Policy (NDCP) 2018.....	24
3.2. M2M/ IoT standardisation in TEC	26
3.2.1. TEC TR - Framework of National Trust Centre (NTC) for M2M / IoT devices and Applications	27
3.2.2. TEC TR - Code of practice for Securing Consumer IoT	27
3.2.3. TEC TR - Recommendations for M2M/ IoT Security	28
3.2.4. Adoption of oneM2M specifications in India	28
3.2.5. Mandatory Testing and Certification of Telecom Equipment (MTCTE)	29
3.2.6. International participation.....	29
3.3. National Critical Information Infrastructure Protection Center (NCIIPC).....	30
3.4. National Security Council Secretariat (NSCS).....	30
3.5. Ministry of Electronics & Information Technology (MeitY).....	30
3.5.1. Standardisation Testing and Quality Certification (STQC).....	31
3.6. MoHUA guidelines on cyber security.....	31
3.7. Bureau of Indian Standards (BIS)	32
3.8. Telecommunications Standards Development Society of India (TSDSI).....	32
4. International study on M2M/ IoT Security – Standards, Regulation & Best practices	33
4.1. ITU standards on IoT Security	33
4.2. ISO/IEC standards on IT/ IoT Security	34
4.3. IEEE guidelines on IoT security.....	34

4.4.	CEN-CENELEC activities on cyber-security	35
4.5.	ENISA -Baseline Security Recommendations for IoT.....	35
4.6.	ETSI Standards on consumer IoT Security	37
4.6.1.	ETSI TS 103 645 - Cyber Security for Consumer Internet of Things.....	37
4.6.2.	International alignment and adoption	38
4.6.3.	ETSI TS 103 848 - Cyber Security for Home Gateways	40
4.6.4.	ETSI initiatives in Quantum - Safe Cryptography.....	40
4.7.	IoT Security Foundation	40
4.7.1.	The Contemporary Use of Vulnerability Disclosure in IoT (Report 4, Nov 2021) 40	
4.7.2.	Consumer IoT Security Quick Guides: No universal default password	41
4.7.3.	IoT Security Assurance Framework (Release 3. 0, November 2021).....	42
4.7.4.	Vulnerability Disclosure Best Practice Guidelines (Release 2.0, Sept 2021)	42
4.7.5.	Secure Design Best Practice Guides (Release 2, December 2019)	42
4.8.	National Institute of Standards and Technology (NIST).....	42
4.8.1.	Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53).....	43
4.8.2.	Consideration for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228)	43
4.8.3.	IoT Device Cybersecurity Guidance for the Federal Government (SP 800-213).....	43
4.8.4.	Foundational Cybersecurity Activities for IoT Devices Manufacturers (NISTIR 8259) 43	
4.8.5.	IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A, May 2020)	44
4.8.6.	Profile of the IoT Core Baseline for Consumer IoT Products (NISTIR 8425, Sept 2022) 44	
4.9.	Global System for Mobile Communications – Associations (GSMA)	44
4.9.1.	IoT SAFE.....	44
4.9.2.	IoT Security Guidelines for Endpoint Ecosystems	46
4.9.3.	Security Features of LTE-M and NB-IoT Networks	46
4.9.4.	IoT Security Guidelines for Network Operators	46
4.9.5.	IoT Security for enterprises: make it work, make it easy	46
4.9.6.	IoT Security Assessment Process	47
4.9.7.	IoT Security guideline for IoT services ecosystem	47
4.9.8.	GSMA eSIM Management IT Infrastructure	47
4.10.	3rd Generation Partnership Project (3GPP)	48
4.11.	GlobalPlatform.....	49

4.12.	Trusted Connectivity Alliances (TCA).....	50
4.13.	Cyber Security Agency, Singapore	50
4.13.1.	The IoT security landscape report.....	50
4.13.2.	Cyber security Labelling Scheme, CSA Singapore	52
4.13.3.	Technical specification -Security Requirements for Residential Gateways...54	
4.13.4.	Technical specification - Security Requirements to guard against Network Storms for Cellular Devices.....	54
4.14.	UK Regulation on Consumer IoT security	54
4.15.	Australian regulation on IoT Security	56
4.16.	USA IoT Bill.....	56
4.17.	Finland Cyber Security labelling scheme	57
4.18.	World Economic Forum (WEF) initiative on IoT Security	57
4.19.	European Union (EU) Cyber security strategy.....	58
5.	Security by Design Guidelines	58
6.	Classification of IoT devices.....	64
6.1.	IoTSF Assurance classes	64
6.2.	TEC TR device classification.....	66
6.3.	Mapping of device classifications / labelling scheme	67
6.4.	Proposed classification for IoT devices in India	70
7.	Testing and certification programme	71
7.1.	ioXt	71
7.2.	Platform Security Architecture (PSA)	72
7.3.	Global Certification Forum (GCF)	73
7.4.	Common Criteria (CC).....	73
7.5.	TrustCB	74
7.6.	GSMA eUICC Security Assurance (GSMA eSA) Scheme.....	74
8.	Summary and Recommendations	75
8.1.	Generic requirements for IoT device security.....	75
8.2.	Hardware security recommendations	77
8.3.	Software security recommendations.....	77
8.4.	Policy related recommendations	78
9.	Abbreviations.....	79
10.	Annexures	80
10.1.	Annexure-I: Important standards.....	80
10.2.	Annexure-II: Some examples of threats and their treatment.....	83

10.3.	Annexure-III: Consumer IoT Vulnerabilities and the relevant capabilities as an example	84
10.4.	Annexure-IV: Use of ITU-T X.509 standard in digital certificates	85
10.5.	Annexure-V: Important links related to e-SIM [Source: GSMA].....	86
	List of virtual meetings of the Working Group.....	87

List of Figures

Figure 1:IoT functional architecture	4
Figure 2 :Components of an IoT Device from security perspective	5
Figure 3 : IoT Product capabilities and developer activities.....	6
Figure 4 : Identity management	9
Figure 5: Challenges to Services and devices with limited capability.....	16
Figure 6: IoT security Factors	17
Figure 7:Vulnerability Disclosure statistics	18
Figure 8: Top countries originating IoT malware infection during 2022.....	21
Figure 9: Summary requirements for IoT Security.....	36
Figure 10 : International Alignments	39
Figure 11:IoT SAFE SIM Architecture	45
Figure 12: IoT SAFE.....	45
Figure 13:GSMA CLP .12 – IoT security Guidelines for service ecosystem.....	47
Figure 14: GSMA SGP.31 eSIM IoT architecture	48
Figure 15:IoT Security challenges vs % of respondent chart	51
Figure 16:CSA labelling scheme	52

List of Tables

Table 1: Vulnerabilities in IoT devices with corresponding threat	20
Table 2: Compliance Classes for IoT Device	65
Table 3 :Classification of devices as per TEC-TR	66
Table 4 : Classification of use cases	67
Table 5 : Revision of table -4 to align with international standards	68
Table 6: Mapping of device classifications from various standardization bodies	69
Table 7:Proposed levels for IoT devices.....	70
Table 8:Consumer IoT Vulnerabilities and the Relevant Capabilities.....	84

List of Contributors

A. Approving Authority:

Name	Designation	Organisation	E-mail Address
R.R. Mittar	Sr. DDG & Head TEC	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

B. Working Group constitution

Designation	Name	Organization	e-mail address
Chairman	Sushil Kumar	TEC	ddgsd.tec@gov.in
Vice Chairman	Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
Vice Chairman	Pranav Singh	Idemia	pranav.singh2@idemia.com
Rapporteur	Prashant Pandey	STMicroelectronics Pvt Ltd.	prashant-mpa.pandey@st.com
Co-Rapporteur & Convenor	Shekhar Singh	TEC	ad.iot-tec@gov.in

C. Authors / Drafting Committee

S.No.	Name	Organization	e-mail address
1.	Sushil Kumar	TEC	ddgsd.tec@gov.in
2.	Pranav Singh	Idemia	Pranav.singh2@idemia.com
3.	Amit Rao	Trusted objects / Device Authority	a.rao@deviceauthority.com
4.	Dinesh Chand Sharma	SESEI	dinesh.chand.sharma@sesei.eu
5.	Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
6.	Prashant Pandey	STMicroelectronics Pvt Ltd.	prashant-mpa.pandey@st.com
7.	Shekhar Singh	TEC	ad.iot-tec@gov.in

D. Participating members

S. No.	Name	Organization	e-mail address
1.	Sushil Kumar	TEC	ddgsd.tec@gov.in
2.	Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
3.	Ms.Namrata Singh	TEC	namrata.singh51@gov.in
4.	Sharad Arora	Sensorise Digital Services / Mashmari	sharad@mashmari.in

S. No.	Name	Organization	e-mail address
5.	Amit Rao	Trusted objects / Device Authority	a.rao@deviceauthority.com
6.	Arvind Tiwary	IoT Forum	arvind_t@sangenovate.com
7.	Prashant Pandey	STMicroelectronics Ltd.	prashant-mpa.pandey@st.com
8.	Aseem Jakhar	Payatu	aseem@payatu.com
9.	Narang kishore	Narnix Technolabs Pvt. Ltd.	kishor@narnix.com
10.	Rahul Singh Jadaan	Rohde & Schwarz India Ltd.	rahulS.Jadaun@rohde- schwarz.com
11.	Dinesh Sharma	SESEI (ETSI)	dinesh.chand.sharma@sesei.eu
12.	Nitin Sharma	SESEI (ETSI)	nitin.sharma@sesei.eu
13.	Vijay Madan	TSDSI	vijay.madan@tsdsi.in
14.	Dr.Vinosh Babu James	Qualcomm	vinosh@qti.qualcomm.com
15.	Dr. R Lenin Raja	AAEMT	dr.lenin@aaemtlabs.com
16.	Ms. Anupama Chopra	CDOT	anupama@cdot.in
17.	Ms. Anjali Jain	STQC	anjali@stqc.gov.in
18.	Ms. Swati Gupta	STQC	swati@stqc.gov.in
19.	A.K. Upadhya	STQC	akupadhyay@stqc.gov.in
20.	Tapas Giri	Taisys	tapas.g@taisys.com
21.	Ms. Arpita Biswas	Databricks, USA	arpitabiswas07@gmail.com
22.	Ms. Kumud Wadhwa	Power Grid	kmd@powergrid.in
23.	Ms. Jyoti Sengar	TEC	jyoti.sengar@gov.in
24.	Gyan Prakash	NSGM	gyan.prakash@powergrid.in
25.	Ms. Parul	ISGF	parul@indiasmartgrid.org
26.	Manoj Belgaokar	SIEMENS	manoj.belgaonkar@siemens.com
27.	Ms. Ashima	TEC	dirsd1.tec@gov.in
28.	Rajneesh Kumar	TEC	Rajneesh.kr@gov.in
29.	Shekhar Singh	TEC	ad.iot-tec@gov.in

E. Editorial Team

S.No.	Name	Organization	e-mail address
1.	Sushil Kumar	TEC	ddgsd.tec@gov.in
2.	Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
3.	Ms. Ashima	TEC	dirsd1.tec@gov.in
4.	Pranav Singh	Idemia	pranav.singh2@idemia.com
5.	Prashant Pandey	STMicroelectronics Pvt. Ltd.	prashant-mpa.pandey@st.com
6.	Ms.Namrata Singh	TEC	namrata.singh51@gov.in
7.	Ms. Riya Soy	TEC	riyasoy221@gmail.com
8.	Shekhar Singh	TEC	ad.iot-tec@gov.in

Executive Summary

IoT / M2M technology is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety, Surveillance, Health care, Agriculture, Smart homes, and Smart cities etc. According to a new market research report published by Markets and Markets, the global Internet of Things (IoT) Security Market size is to grow from USD 12.5 billion in 2020 to USD 36.6 billion by 2025, at CAGR of 23.9 percent during the forecast period¹. Security of the IoT domain, from devices to the applications becomes a matter of paramount importance as hacking of the devices / network being used in daily life will harm companies, organisations, nations and more importantly people. It may result in collapse of the services, creating panic and may result in chaos. Ensuring end to end security for connected IoT devices is key to the success for this market - without security, IoT will cease to exist. Privacy of the data of the individual is very important especially in the health care domain.

IoT devices, services and software, and the communication channels that connect them, are at risk of attack by a variety of malicious parties, from novice hackers to professional criminals or even state actors. Possible consequences to consumers of such an attack could include:

- Loss of device functionality
- Impact on Individuals, community, and risk to the nation
- Inconvenience and irritation
- Infringement of privacy
- Loss of life, money, time, property, health, relationships, etc.

For vendors, operators and suppliers, potential consequences may include loss of trust, damage to reputation, compromised intellectual property, financial loss and possible prosecution.

Malicious intent commonly takes advantage of poor design, but even unintentional leakage of data due to ineffective security controls can also bring dire consequences to consumers and vendors. Thus, it is vital that IoT devices and services have security designed in from the outset.

World Economic Forum (WEF) in its report titled *Future of Connected World*¹, released in June 2022, mentioned that there was an increase in Cyber attacks by 31% in 2021 as compared to 2020 and also the IoT device attacks became double in the first half of 2022 as compared to 2021.

A reference was sent by DoT vide its letter dated 05th Jan 2016 seeking the recommendations of Telecom Regulatory Authority of India (TRAI) on three aspects related to M2M communications i.e., Quality of Service in M2M Services, M2M Roaming Requirements and M2M Spectrum Requirements.

To address the requirements sent by DoT, TRAI released its recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine Communications' September

¹https://www3.weforum.org/docs/WEF_Future_of_the_Connected_World_2022.pdf

2017 (available on TRAI website <https://traai.gov.in>). These recommendations were accepted by the Digital Communication Commission.

Following work items (recommendations) were communicated to TEC by DoT, vide L.No. 6-18/2018-Policy I dated 1st October 2018, to develop the security framework for the IoT ecosystem in the country:

1. Device manufacturers should be mandated to implement “Security by design” principle in M2M devices manufacturing so that end to end security can be achieved.
2. A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software).

However, DoT also decided that 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 Centre.

To address the work items mentioned above, a multi-stakeholders working group was formed in TEC with the approval of Sr.DDG, TEC to study the national / international scenario, available standards and best practices across the globe and submit its recommendations.

Two Technical Reports² as a part of this document namely ***Code of Practice for Securing Consumer IoT*** and ***Framework for National Trust Centre*** have been released in August 2021 and March 2022 respectively (More details are in section 3.2).

Testing and certification of telecom equipment and the IoT devices have already been started in phased manner based on the Essential Requirements (ERs) prepared under TEC MTCTE regime notified by DoT in September 2017 (details in section 3.2.5).

This document is intended to be used by the following stakeholders:

- **M2M/ IoT Device Manufacturers** who manufacture IoT devices.
- **M2M/ IoT Application Developers** who develop IoT applications for provisioning of IoT services.
- **M2M/ IoT System Integrators** who integrate different components for provisioning of services.
- **M2M/ IoT Service Providers** who provide solutions to customers as per their requirements in different verticals such as smart homes, smart cities, automotive, transport, health, utilities, and consumer electronics. M2M/IoT service providers will also have the platform for connecting IoT devices directly or through Gateway.

²<https://tec.gov.in/M2M-IoT-technical-reports>

- **Communication Network Operators** who provide communication services to IoT Service Providers for connecting the devices/ gateways.
- **Policy makers** responsible for preparing related policies for the proliferation of M2M/ IoT ecosystem.

This document covers the national / international standards, policies and the best practices important for the development of secured IoT devices. Additionally, the document contains recommendations in section 8 for ensuring the security of such devices.

1. Introduction to M2M/ IoT

M2M refers to the technologies that allow devices to communicate with each other via wired / wireless systems. 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 another device running an application (software program), that translates the captured event into meaningful information. The enabling technologies for M2M are sensor networks, RFID, mobile Internet, wired & wireless communication networks, IPv4 / IPv6, etc.

The IoT ecosystem may have M2M devices, Gateways, Communication technologies, Big data and Process management, IoT platform, User interface (web, Mobile, HMI) etc. Security is required to be an integral part of the IoT ecosystem. Figure-1 illustrates the IoT functional architecture.

The Internet of Things (IoT) is the network of physical objects that contain embedded technology to sense and communicate or interact with internal states or the external environment through internet-based communication technologies.

Any stand-alone internet-connected device that can be monitored and/or controlled from a remote location could be considered an IoT device.

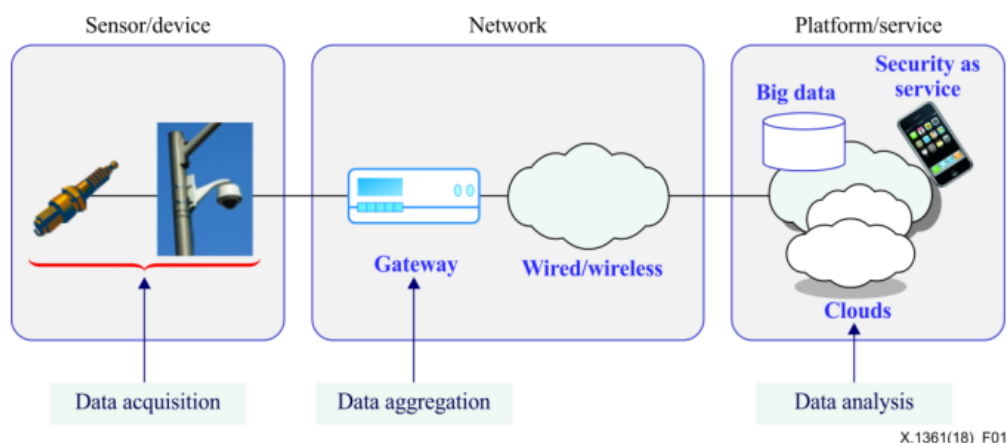


Figure 1:IoT functional architecture³

ITU-T in its Recommendation ITU-T Y.4000/ Y.2060 (06/2012) 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.

The Internet of Things (IoT) is revolutionizing and changing the way businesses, governments, and consumers interact with the physical world. This level of disruption has a significant impact on the world in improving the quality of life.

³<https://www.itu.int/itu->

[t/recommendations/rec.aspx?id=13607#:~:text=Recommendation%20ITU%2DT%20X.,mitigate%20these%20threats%20and%20challenges.](https://www.itu.int/itu-t/recommendations/rec.aspx?id=13607#:~:text=Recommendation%20ITU%2DT%20X.,mitigate%20these%20threats%20and%20challenges.)

In view of the envisaged impact and humongous growth, Security considerations become an integral part of the IoT Ecosystem.

1.1. IoT Device

IoT devices are extremely varied in nature and may consist of some, or all of the components depicted in figure-2 below:

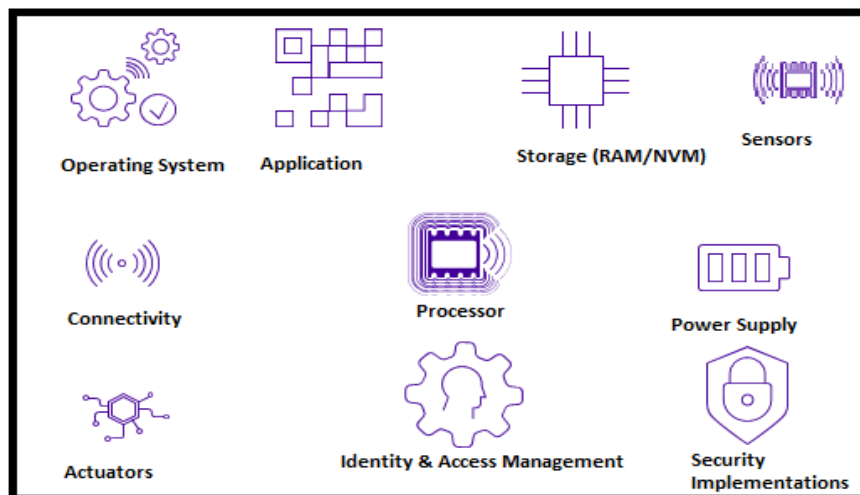


Figure 2 :Components of an IoT Device from security perspective

Sensors and actuators are the fundamental elements of IoT device, which may have limited processing capability and storage controlled by an operating system with a dedicated application, connected to the backend system through various communication technologies, wired / wireless, depending upon the use case requirements. And last but not the least, it also has a power supply module or battery to energise it. The composition of an IoT device can vary – it can be a simple sensor with a minimal firmware, or a stand-alone appliance with a full-fledged operating system (OS), IoT devices can also be things that implement fully functional web servers.

IoT devices are often resource-constrained. Many of the IoT devices use a microcontroller rather than a full-fledged microprocessor and run at a few hundred MHz rather than GHz. An IoT device may be as advanced as a connected car with a powerful Electronic Control Units (ECUs) or a simple temperature-monitoring device. Communication technology play an important role in connecting the devices with the headend system /platform. The various communication technologies being used in M2M / IoT domain have been elaborated in the TEC Technical Reports as listed below:

1. **Communication technologies in M2M/ IoT domain⁴** released in 2017 has detailed the cellular technology (up to LTE 3GPP release 14), Low power wireless communication technologies, Low power wide area network technologies (LoRA , SigFox, NB-IoT, LTE-M etc.), IEEE 802.11 a, b, g, n, ac (variant of WiFi), 802.11p (DSRC), wire line (PLC, DSL,

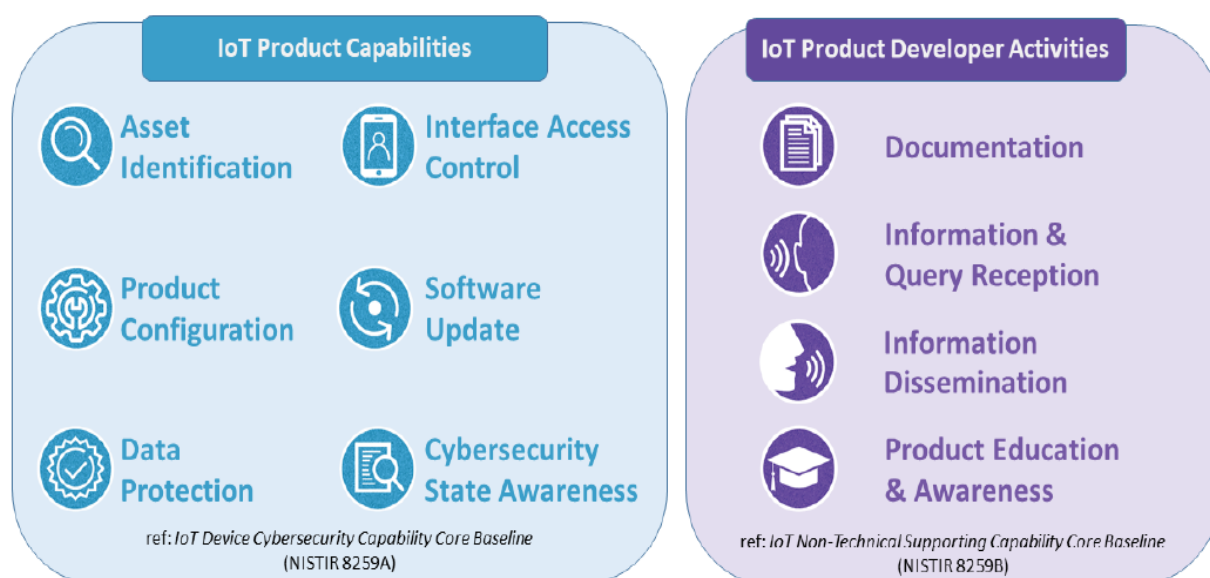
⁴<https://tec.gov.in/pdf/M2M/Communication%20Technologies%20in%20IoT%20domain.pdf>

FTTH) etc. and the related use cases such as smart lighting solutions in smart cities, smart metering etc.

2. **Emerging Communication Technologies and Use cases in IoT domain**⁵ released in 2021 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.

1.2. IoT Product requirements and developer's initiative

In view of massive growth of connected devices, security of the IoT ecosystem is a major concern to avoid hackings/ tampering related issues. It is necessary to define the cyber security related capabilities requirement for IoT devices and the initiatives to be taken by the designer/ developer of these products. Figure-3 illustrates the high-level capabilities required for the IoT product and related activities on the part of developer/ designer.



[source:NIST IR 8425⁶]

Figure 3 : IoT Product capabilities and developer activities

IoT product capabilities have been described below from the cybersecurity utility point of view:

⁵<https://tec.gov.in/pdf/M2M/Emerging%20Communication%20Technologies%20&%20Use%20Cases%20in%20IoT%20domain.pdf>

⁶ <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf>

I. Asset Identification

Unique identification of all IoT products and their components is necessary to support the activities such as asset management for updates, data protection, and digital forensics capabilities for incident response besides establishing accountability associated with the device.

II. Product Configuration

The configuration of the IoT product should be changeable, with the ability to restore a secure default setting, and any changes can only be performed by authorized individuals, services, and other IoT product components.

Using this ability, Customer should be able to configure the IoT products to avoid specific threats and risk based on their risk appetite. The Customer, authorized individuals and other IoT product components should also have the capability to revert/ restore the IoT product to a secure default setting.

III. Data Protection

Maintaining confidentiality, integrity, and availability of data is foundational to cybersecurity for IoT products. Each IoT product component shall be able to protect the data including stored data, via secure means.

IV. Interface Access Control

Controlling access to internal and external interfaces to preserve the confidentiality, integrity, and availability of the components by preventing unauthorized access and breach of security.

V. Software Update

Software may have vulnerabilities discovered after the IoT product has been deployed; software update capabilities can help ensure secure delivery of security patches.

VI. Cybersecurity State Awareness

This capability may be achieved in the IoT products by supporting the detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit. Protection of data and ensuring proper functionality can be supported by the ability to alert the customer when the device starts operating in unexpected ways. IoT product developer/ designer is expected to build up these capabilities within the IoT product. (More details about NIST standards are available in section 4.8).

Based on above capabilities it becomes important to establish a chain of trust involving a hardware-based root of trust (device identity, secure element etc.), secure boot loader, operating system and applications.

Device software has to check the integrity of software and hardware assets (Boot loader, Operating System, Applications) during the boot process. Secure Boot is required to be considered at the design level of IoT device.

Side channel attack is one of the major concerns resulting from weak implementation of security. To exploit algorithm and operating system activity, attackers use techniques such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA) to perform side-channel attacks on IoT devices. It is therefore imperative for IoT device developers to integrate robust security measures that can safeguard against such attacks.

1.2.1. Identity management for M2M/IoT devices

The IoT product capabilities have been depicted in figure-3. The ITU-T recommendation Y.2060 on *Next Generation Network: Frameworks and functional architecture models* has defined four layers in IoT reference model namely Application layer, Service support application support layer, Network layer and Device layer associated with management capabilities. The IoT reference model, IDM (Identity Management) functions and IoT product capabilities are key implementations to secure and manage the IoT device lifecycle. In connected ecosystem with legacy framework, various identifiers with respect to the technology are available, e.g. in cellular technology IMEI is a GSM application identifier, MEID/ESN is a CDMA application Identifier and MAC address is generally for identification of devices used in non-cellular technologies.

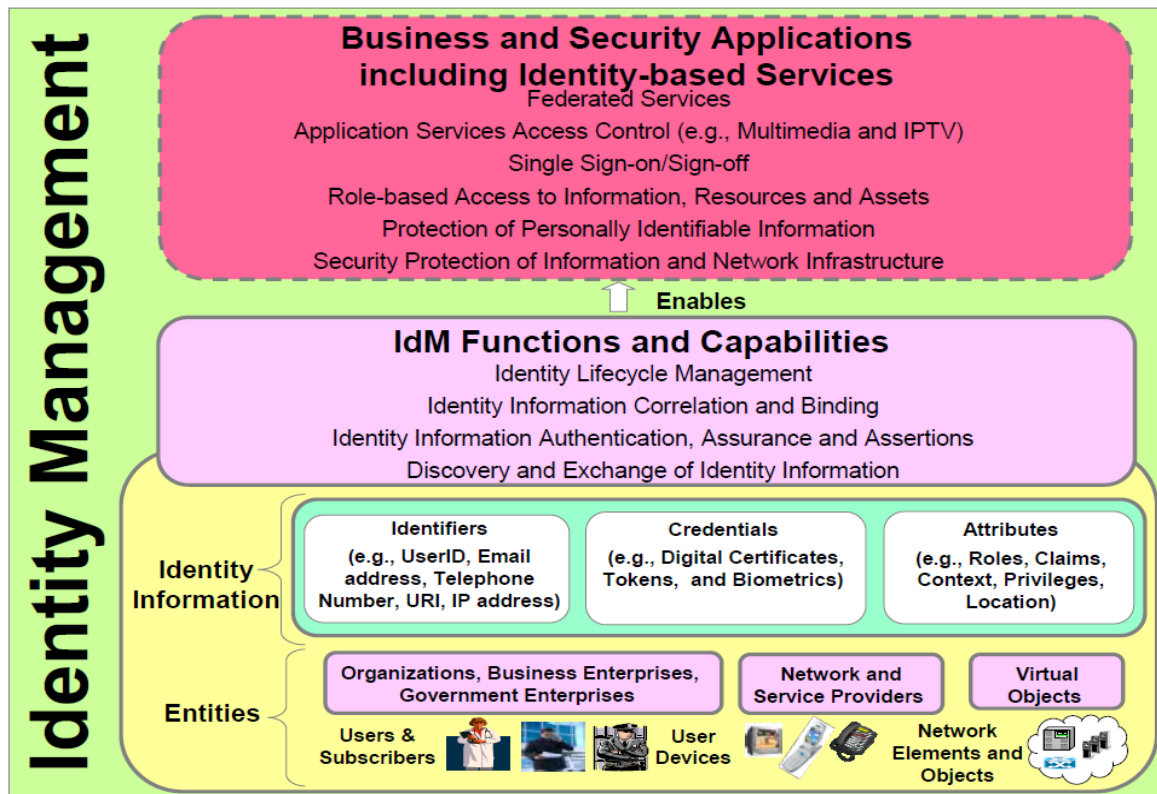
Understanding the criticality and scope of Identity management, ITU-T Y.2720 (*NGN Identity Management Framework*) addresses below requirements with respect to the Identity:

- Assurance of identity information,
- Assurance of the identity of an entity,
- Enabling business and security applications

Identity information associated with an entity can be grouped as follows:

- Identifiers (e.g., UserID, e-mail addresses, telephone numbers, URI and IP addresses).
- Credentials (e.g., Digital certificates, tokens, and biometrics)
- Attributes (e.g., Roles, claims, privileges, patterns, and location).

It has been illustrated in the figure-4 below :



[Source: ITU –T Y. 2720]

Figure 4 : Identity management

IDM (Identity Management) enables the security of various applications such as

- **Business Application**
 - ❖ Access to multiple applications and services without having to individually authenticate each application or service platform
 - ❖ Access to services across different service providers or NGN providers)
- **Identity-based Services**
 - ❖ Identifier, credential, and attribute services
 - ❖ bridging services (mapping and interworking of identity information in a heterogeneous environment)
 - ❖ Pattern information services
- **Security applications**
 - ❖ Access control for network and application services (e.g., VoIP, IPTV and data)
 - ❖ Role-based access control to information, resources, and assets
 - ❖ Authorization and privilege management
 - ❖ Application layer security along with the Transport layer security e.g. HTTPS (HTTPS uses TLS (SSL) to encrypt normal HTTP)

IDM function capabilities may be enhanced with the following concepts:

- a. **Secure Identifier:** Identities e.g. MEID, IMEI, ESN, MAC etc., which are exposed and thus vulnerable, may be the first choice of attackers to steal it. Identity management services can ensure the security of device identifier.

Secure identifier configuration can be created uniquely for IoT device, which can be generated during on boarding or enrolment process of IoT devices. That generated identity should be stored in tamper-proof environment, and strictly confidential between IoT devices and their respective platforms.

- b. **Security Module:** This module contains the algorithm and security keys for symmetric or asymmetric encryption and decryption using Public Key Infrastructure (PKI) for cryptography algorithm. PKI comprising of Public and private keys pair is employed to encrypt and digitally sign the data. In IoT devices, these keys are usually contained inside an ITU-T X.509 digital certificate, which is installed in the device in a secure tamper-proof environment during manufacturing by the manufacturer or during provisioning of the device by the system integrator/installer. The certificate is certified and signed by a trusted authority. The advantage of ITU-T X.509 is a hierarchical format that along with the public key contains information like certificate validity, usage and details of the issuing authority that can be used for device life cycle management⁷.

For the constrained IoT devices, the National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize **Lightweight Cryptographic** algorithms. For this NIST had selected a group of cryptographic algorithms, known as *Ascon*⁸, to be the formal encryption standard for "lightweight" electronic devices and their communications e.g. medical devices, stress detectors on roads and bridges, and keyless entry fobs for cars.

1.3. IoT Device – Security Challenges

The IoT devices deployed in the network may have following complexities & Security challenges:

1. IoT products are generally deployed in insecure or **physically exposed environments**.
2. Security is new to many manufacturers and there is **limited security planning and weak architecture for operating system, application including** development methodologies. It is generally taken as the last item in the development process.
3. The majority of IoT devices have limited capabilities, e.g., processing, memory and power, and therefore advanced security controls cannot be effectively applied at the device.

⁷<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>

⁸<https://www.darkreading.com/ics-ot/nists-new-crypto-standard-a-step-forward-in-iot-security>

4. **Due to the fragmentation of standards & regulations and their lack** of availability / acceptability, it becomes difficult for the device manufacturers to decide which standard to follow.
5. **The widespread deployment** apart from commercial applications of IoT, recent trends have seen Critical Legacy Infrastructures (CLIs) migrating toward IoT based monitoring and control.
6. **Security integration** is a very challenging task, due to the requirements from all involved stakeholders. Presence of a single insecure IoT device can be threatening to the security of entire network.
7. In view of threats and security-related challenges in IoT domain across the globe, expertise is required to be built-up and updated time to time.
8. Secure update for firmware and operating system is a challenging task due to lack of secure OTA support in device capabilities.
9. Secure Architecture for Hardware abstract layer may be missing in embedded firmware for native Operating system for IoT segment.
10. Absence of common methodology for Information Technology Security Evaluation in IC platform protection profile.

2. Attacks, Vulnerabilities, Threats in IoT domain and Risk mitigation

2.1. Cyberattacks

IoT based solutions have been used across the globe to create Smart infrastructure in various sectors namely energy, transportation, banking, critical services, water management, Smart homes, Smart cities etc. With the increase in IoT based solutions, networks and internet connections, these systems are subject to vulnerability and digital attack. Cyber-attack in any critical infrastructure may be catastrophic. Some of the IoT based cyber-attacks on critical infrastructure across the globe are listed below:

1. In February 2021, an unknown hacker or group of hackers was able to gain access to the operations technology (OT) system of a water treatment plant in Oldsmar, Florida. The attack attempted to poison the water supply by increasing the amount of sodium hydroxide, also known as lye, in the water from 100 parts per million to 11,100 parts per million⁹.
2. In June 2020, Cyber-attack hit all US mobile phone operators sparking outages¹⁰. T-Mobile, AT&T, Verizon, and Sprint customers reported outages in areas including Florida, Georgia, New York, and California on Monday afternoon. The disruptions were part of a large-scale distributed denial-of-service, or DDoS, attack

⁹<https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=f980fdf28e7c>

¹⁰<https://www.thesun.co.uk/news/11871782/ddos-attack-t-mobile-outage-facebook-instagram-us/>

meant to overwhelm an online service with multiple traffic sources to render it unusable, according to Pop Culture.

In June 2020, website down detector¹¹ reported about the widespread outage in T-mobile network affecting around 100,000 T-Mobile customers¹².

3. Cyber security attack in Ukraine: -

- (i) In December 2015, hackers using the Black Energy malware remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to 230,000 consumers¹³.
- (ii) In December 2016, power grid was hacked by the cyber attack “Industroyer” malware to sabotage the critical infrastructure by hacking the SCADA system¹⁴. There was a massive power outage affecting 225,000 consumers for several hours. The cyber-security company Information Systems Security Partners (ISSP) linked the incident to a malware-based cyberattack.
- (iii) In March 2022, “Indusroyer 2” malware attack was traced which resulted in power outage in Ukraine¹⁵.

4. In 2017, Cable News Network (CNN) wrote, “The FDA confirmed that St. Jude Medical’s implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks¹⁶.”

5. In 2017, in Saudi Arabia a cyber-attack Triton was traced¹⁷, which was vulnerable for safety and human life.

6. Water Company Hacking (USA, 2016):- The attackers infiltrated water utility’s SCADA system and managed to manipulate the system to change the amount of chemicals used. In this way they intervened in water treatment and production¹⁸.

7. Smart Building Attack (Finland, 2016):- Smart homes and buildings use IoT devices for various applications. This DDoS attack shut down heat and hot water systems in two

¹¹<https://downdetector.com/status/t-mobile/>

¹²<https://mashable.com/article/widespread-outages-t-mobile-att-verizon-sprint>

¹³[https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_\(2015\)](https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015))

¹⁴[https://cyberlaw.ccdcoe.org/wiki/Industroyer_%E2%80%93_Crash_Override_\(2016\)](https://cyberlaw.ccdcoe.org/wiki/Industroyer_%E2%80%93_Crash_Override_(2016))

¹⁵<https://www.headmind.com/fr/industroyer-2/>

¹⁶<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities>

¹⁷<https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton#:~:text=In%20December%202017%2C%20newly%20discovered,safety%20systems%20in%20critical%20infrastructures.>

¹⁸https://www.theregister.com/2016/03/24/water_utility_hacked/

buildings in winter of Finland. The DoS attack flooded the building control system with bogus internet traffic which resulted in restarting of the system every few minutes and denying administrator's remote access to the device¹⁹.

8. BMW connected car vulnerability:- A security vulnerability in BMW's Connected Drive system allowed researchers to unlock the vehicles without the car keys²⁰. The attack took advantage of a feature that allows drivers who have been locked out of their vehicles to request the remote unlocking of their car from a BMW assistance line. The researchers were able to impersonate BMW servers and send, over the public cellular network, remote unlocking instructions to vehicles. The software patch for the 2.2 million cars equipped with connected drive adds HTTPS encryption to the connection from BMW to the car and ensures that the car only accepts connections from a server with the correct security certificate.
9. Mirai DDoS:- Mirai gathered a botnet made up of more than one million hacked IoT devices, mostly DVRs and CCTV cameras, which were infected through their Telnet port. The French hosting company OVH is believed to be the first to have suffered a DDoS attack coming from the Mirai botnet, which was reported to have peaked at 1 Tbps, one of the largest recorded in history in terms of volume. Just a day after the attack against OVH, the Mirai botnet conducted a DDoS attack on "Krebs on Security" website that surpassed 620 Gbps of traffic, making it also one of the largest recorded in history in terms of volume.

Similar attack happened in October of 2016, on service provider Dyn using an IoT botnet. This led to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN. This botnet was made possible due to malware named Mirai²¹. Mirai botnet targets IoT devices and scans the web to find poorly secured IoT devices that still have default usernames and passwords.

10. Light Rail System Attack, San Francisco 2016: The light rail system in the USA was subjected to a ransomware attack in the year 2016 by clicking a phishing mail in the system²².
11. Foscam IP Baby-Cam hijacked: - In 2013, a vulnerability in Foscam wireless cameras was disclosed by security researchers in a presentation titled "To watch or to be watched: Turning your surveillance camera against you". Later on an attacker gained control of one of those cameras in Houston, Texas, which was being used as a baby-cam. The attacker was able to see, hear and speak through the camera²³.

¹⁹<https://www.bleepingcomputer.com/news/security/ddos-attacks-bring-down-heating-system-for-two-buildings-in-small-finnish-town/>

²⁰<https://www.computerworld.com/article/2878424/bmw-cars-found-vulnerable-in-connected-drive-hack.html#:~:text=A%20security%20vulnerability%20in%20BMW's,several%20models%20of%20BMW%20cars.>

²¹<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities>

²² <https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/>

²³ <https://time.com/79170/stranger-hacks-into-baby-monitor-and-screams-at-child/>

12. Saudi Arabia faced a cyber-attack as a wiper malware, in 2012, further it was named as Saudi Aramco²⁴.
13. In 2010, Iran faced a cyber-attack known as Stuxnet, which had targeted industrial operations²⁵.
14. In 2009, the Puerto Rican Electric Power Authority (PREPA), US territory, suffered a series of power theft incidents related to its smart meter deployment. The attack required physical access to the smart meters, and it is believed that former employees of the meter manufacturer were altering the smart meters to reduce power bills. It costed the Puerto Rican Electric Power Authority as much as \$400 million a year.

This attack was largely successful, as many people did not change the default logins of their devices. Numerous websites such as Twitter, Netflix, Spotify, and Reddit could not be available for a day. A Botnet is a network of systems combined together with the purpose of remotely taking control and distributing malware. Controlled by botnet operators via command-and-control-servers, they are used by criminals on a grand scale for various purposes such as stealing information, exploiting online-banking data, Distributed Denial of Service (DDoS) - attacks or for spam and phishing emails.

15. Federal Bureau of Investigation (FBI) issued warning in 2019 that smart TV may be vulnerable to intrusion. Malicious actors can change channels, play with the volume, and control the Smart TV. In a worst-case scenario, they can turn on camera and microphone of the Smart TV and silently cyberstalk.
In order to guard against possible intrusion, **the FBI recommended that smart TV users educate themselves on their device's security settings, change default network passwords set by manufacturers, and understand how to enable and disable microphones and cameras**²⁶.
16. Server at All India Institute of Medical Science (AIIMS), Delhi was hacked²⁷ in Dec 2022 causing disruption in services and compromise of data as reported by Mint. The cause of disruption is said to be the malware infection.
17. Some computers in DoT-Controller of Communication Accounts (CCA), Vijayawada, India came under suspected ransomware attack²⁸ in Jan 2023.

²⁴ <https://journals.nauss.edu.sa/index.php/JISCR/article/download/455/979/5742>

²⁵ <https://www.microsoft.com/en-us/security/business/security-insider/cyber-signals-1/the-convergence-of-it-and-ot/>

²⁶ <https://edition.cnn.com/2019/12/02/politics/smart-tv-fbi-warning-cyber-monday/index.html>

²⁷ <https://www.livemint.com/news/india/aiims-cyber-attack-puts-digital-health-id-plan-under-scanner-11671473243687.html>

²⁸ <https://timesofindia.indiatimes.com/city/vijayawada/cyberattack-on-cca-system/articleshow/96805771.cms>

18. In February 2020, Computer Emergency Response Team, India (CERT-in)²⁹ issued warning for the users of video conferencing app *Zoom* that is prone to cyber-attacks, mentioning about the existence of vulnerability in Zoom due to weak authentication methods used by Zoom during video conferencing. Successful exploitation of this vulnerability could allow a remote attacker to join active video conference and obtain sensitive information such as documents, presentations etc. In July 2019, Indian Computer Emergency Response Team(www.cert-in.org.in) issued a warning about the new malware named as "Silex" targeting IoT devices. The malware was capable of trashing an IoT device's storage, dropping firewall rules, removing the network configuration, and then halting the device.

From the incidents mentioned above following basic points may be considered for IoT security:

- Devices connected to the public network that cannot have their software, passwords, or firmware updated should never be used.
- Changing the default username and password should be mandatory during the installation of any network connected device.
- Passwords for IoT devices should be unique per device, especially when they are connected to the Internet.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities.

2.2. IoT - Threats & Vulnerabilities

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks. In particular, there may be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves³⁰.

IoT systems are based on two main components- system hardware and system software, and both have design flaws quite often. Hardware vulnerabilities are very difficult to identify and difficult to fix. Software vulnerabilities can be found in operating systems, application software, and control software like communication protocols and devices drivers.

As per Open Web Application Security Project (OWASP) top 10 IoT vulnerabilities are:

1. Weak, Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism

²⁹<https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-0023>

³⁰https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

In view of the various hackings / attacks on IoT networks, IoT security is the prime need to safeguard connected devices and networks in IoT domain. Allowing devices to connect to the internet opens them to a number of serious threats if they are not properly secured.

In addition to conventional security solutions, there is need to provide built-in security in devices for dynamic prevention, detection, diagnosis, isolation, and counter measures against successful breaches.

Figure-5 illustrates the security and service challenges related to IoT device and how to protect the devices

IoT device protection against Security challenges

AVAILABILITY	IDENTITY	PRIVACY	INTEGRITY
Ensuring constant connectivity between Endpoints and their respective services	Authenticating Endpoints, services, and the customer or end-user operating the Endpoint	Reducing the potential for harm to individual end-users.	Ensuring that system integrity can be verified, tracked, and monitored.

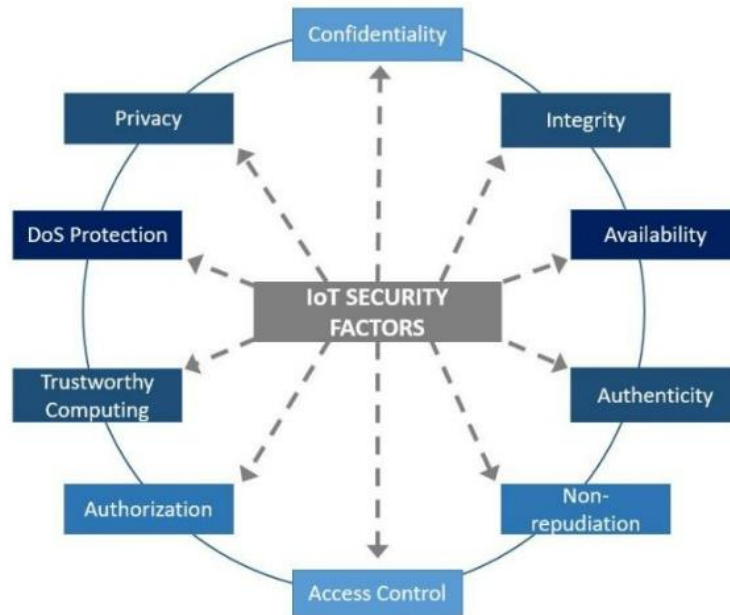
IoT device Service challenges

LOW COMPLEXITY	LOW POWER	LONG LIFECYCLES	PHYSICALLY ACCESSIBLE
<ul style="list-style-type: none"> ➔ Low processing capability. ➔ Small amounts of memory. ➔ Constrained operating system. 	<ul style="list-style-type: none"> ➔ No permanent power supply ➔ Possibly permanent, but limited power supply. 	<ul style="list-style-type: none"> ➔ Requires cryptographic design that lasts a lifetime. ➔ Manage security vulnerabilities which can't be patched within the endpoint. 	<ul style="list-style-type: none"> ➔ Access to local interfaces inside the IoT endpoint. ➔ Hardware components and interfaces potential target of attackers.

[Source: GSMA | Resource Library | Internet of Things]

Figure 5: Challenges to Services and devices with limited capability

To address the various threats and vulnerabilities related issues, a number of security requirements have been identified. The key points have been mentioned in the figure-6:



[source: <https://iotac.eu/9-important-security-requirements-to-consider-for-iot-systems/>]

Figure 6: IoT security Factors

Vulnerability management is one of the most basic tenets of security, and all IoT manufacturers are expected to disclose the vulnerabilities in their products as and when they are discovered. For this a proper mechanism is required to be built-in. IoT Security Foundation in its report *The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2022*³¹ released in 2023, mentioned that in year 2022, only 27.11% of the companies had a vulnerability disclosure policy. This is up from 21.6% in 2021, 18.9% in 2020, 13.3% in 2019, and 9.7% in 2018 as illustrated in the figure-7. The increase has been an average of approximately 4.3% each year. This document has also mentioned that if this rate of adoption continues, 100% compliance will not be reached until 2039.

³¹<https://www.iotsecurityfoundation.org/wp-content/uploads/2023/01/IoTSF-Release-The-State-of-Vulnerability-Disclosure-Usage-in-Global-Consumer-IoT-in-2022.pdf>

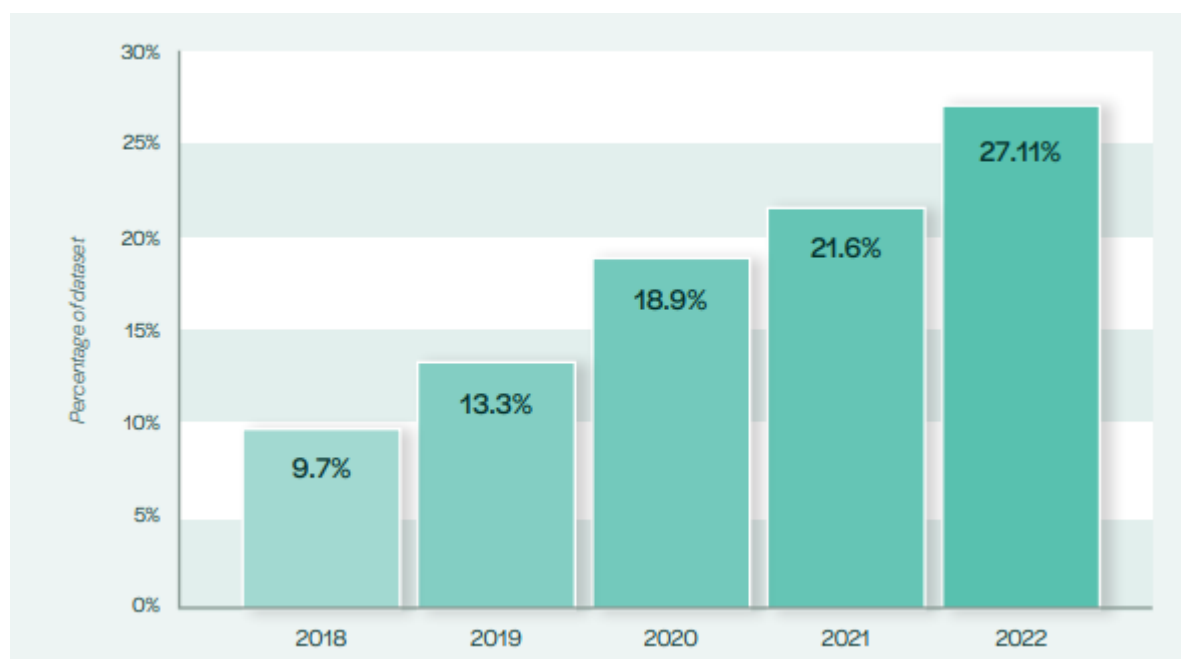


Figure 7: Vulnerability Disclosure statistics

Table below details the vulnerabilities in IoT devices with corresponding threat.

S.No.	Threat	Vulnerabilities
1.	Vulnerable device - Operating System and Application software	IoT devices rely on software that might contain poor design choices and/or security bugs such as buffer overflows and improper exception handling. This makes them vulnerable to many attacks that can compromise data confidentiality or integrity
2.	Privacy threat	Device location and usage pattern tracking poses a privacy risk to users; an attacker can infer sensitive information from data gathered and communicated by devices. Such information may be sold to interested parties for marketing purposes or used for unauthorised surveillance.
3.	Eavesdropping	Communication over an IoT network can be intercepted and deciphered if the communication channel is not sufficiently protected, for instance if keying material, security parameters, or configuration settings are exchanged or if weak or unsuitable cryptographic algorithms are used. Related attacks include man-in-the-middle, session hijacking, or message replay
4.	Denial of Service (DoS)	Many devices, being resource-constrained, are susceptible to denial-of-service attacks launched by attackers sending continuous requests to deplete device resources. On the other hand, compromised devices can themselves be used to disrupt the operation of other networks or systems via a Distributed DoS (DDoS) attack

5.	Insecure Firmware-upgrade or outdated firmware	An attacker may be able to replace device firmware during device commissioning or under the guise of a routine upgrade. IoT device may be compromised in case the firmware is outdated. In a related attack, the attacker downgrades the firmware to a legitimate but less secure version.
6.	Malware	Software programs designed to carry out unwanted and unauthorised actions on a system without the consent of the user, resulting in damage, corruption, or information theft. Its impact can be high. Devices can be infected with programs designed to carry out unauthorised actions on a system, possibly using existing vulnerabilities in software or firmware.
7.	Exploit Kits	Code designed to take advantage of a vulnerability to gain access to a system. This threat is difficult to detect and in IoT environments its impact ranges from high to crucial, depending on the assets affected
8.	Targeted attacks (APT)	Attacks designed for a specific target, launched over a long period of time, and carried out in multiple stages. The main objective is to remain hidden and to obtain as much sensitive data/information or control as possible. While the impact of this threat is medium, detecting them is usually very difficult and takes a long time.
9.	Counterfeit devices	Counterfeited devices may introduce series problems for all market sectors, starting from the end user to vendors. Moreover, adverse consequences of counterfeit devices could affect governments and private sectors. For electronic devices, there are several anti-counterfeiting such as Electronic Product Code (EPC) and International mobile equipment identity (IMEI).
10	Use of weak encryption algorithm	A majority of the weak certificates belong to Internet-connected devices such as routers and modems with limited resources on them in terms of processing power, memory, and entropy. Designers of IoT devices need to pay closer attention to the encryption available on their devices. They need to be thinking about how to add entropy to the process.
11.	Man in the middle	Active eavesdropping attack, in which the attacker relays messages from one victim to another, to make them believe that they are talking directly to each other, while intercepting and potentially tampering the messages.
12.	IoT communication protocol hijacking	Taking control of an existing communication session between two elements of the network. The intruder can sniff sensible information, including passwords. The hijacking can use aggressive techniques like forcing disconnection or denial of service.

13	Interception of information	Unauthorised interception (and sometimes modification) of a private communication, such as phone calls, instant messages, e-mail communications
14.	Replay of messages	This attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, to manipulate or crash the targeted device.
15.	Software vulnerabilities	The most common IoT devices are often vulnerable due to weak/ default passwords, software bugs, and configuration errors, posing a risk to the network. This threat is usually connected to others, like exploit kits, and it is considered crucial.
16.	Third party's failures	Errors on an active element of the network caused by the misconfiguration of another element that has direct relation with it.
17.	Device modification	Tampering a device by for example taking advantage of bad configuration of ports, exploiting those left open.
18.	Device cloning or substitution	Device cloning or substitution A non-trusted factory can clone the physical characteristics, firmware/ software, and security configuration of the device.
19.	Data leakage	Disclosure of sensitive data, intentionally or unintentionally, to unauthorised parties. Confidential data may be captured by an attacker from individual devices, during transit, or from the backend.
20.	Weak user/admin credentials and authentication	Poor credential management such as weak password choices and lack of multi-factor authentication for the user and administrative interfaces of devices, gateways or back-ends is a common vulnerability in many information systems including IoT.
21.	Lack of Physical Hardening	<p>Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.</p> <p>Because of the ubiquity of IoT computing, devices are usually not kept in a secure location but must be exposed in the field to perform their tasks. In the absence of surveillance, this could easily allow malicious actors to tamper with or access devices.</p>

Table 1: Vulnerabilities in IoT devices with corresponding threat

Some examples related to threats and their treatment are given in the annexure-II.

Microsoft in its third edition of Cyber Signals³², December 2022, published a list of countries generating malware infection from the connected devices during 2022 as illustrated in the figure-8 below. As per this report, India is at the third place, after China and US, in countries originating malware infection during 2022.

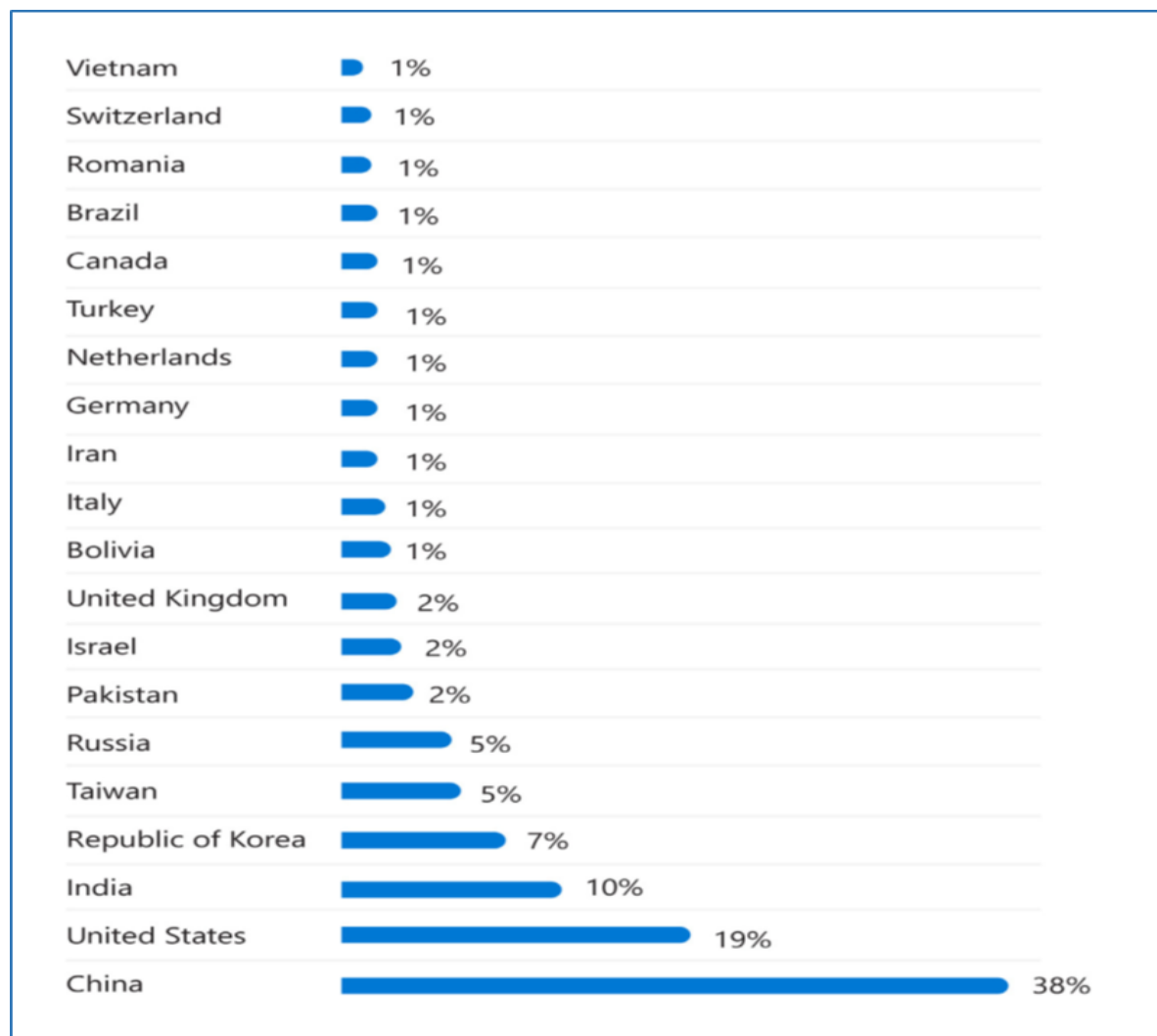


Figure 8: Top countries originating IoT malware infection during 2022

2.3. Risk Mitigation Areas

Cybersecurity risks for IoT devices can be thought of in terms of two high-level risk mitigation goals³³:

1. **Protect device security:** It is necessary that a device should not act as means for conducting attacks, including participating in DDoS attacks against other

³²<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5daTD>

³³<https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline>

organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.

2. **Protect data security:** Protect the confidentiality, integrity, and/or availability of data (including personally identifiable information [PII]) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device except those without any data that needs protection.

The Common risk mitigation areas for IoT devices are:

1. **Asset Management:** Maintain a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices' lifecycles to use that information for cybersecurity risk management purposes.
2. **Vulnerability Management:** Identify and eliminate known vulnerabilities in IoT device software and firmware to reduce the likelihood and ease of exploitation and compromise (more details in section 4.7.1).
3. **Access Management:** Prevent unauthorized and improper physical and logical access to, usage of, and administration of IoT devices by people, processes, and other computing devices.
4. **Data Protection:** Prevent access to and tampering with data at rest or in transit that might expose sensitive information or allow manipulation or disruption of IoT device operations.
5. **Security keys protections:** Encryption is the essence of security of IoT devices. The use of symmetric and/ or asymmetric key is done based on the use case. Besides the robustness and strength of the encryption, the storage and management of the keys used for encryption are matters of utmost importance. It is essential that these cryptographic keys are stored in tamper proof environment.
6. **Incident Detection:** Monitor and analyze IoT device activity for signs of incidents involving device and data security.
7. **Zero Trust Security implementation:** Zero trust security model is based on the principle of "never trust, always verify". Zero Trust requires that user and device access privilege be continuously verified even after authentication. The latest knowledge about cyber threats is required to be incorporated into the IoT device protection and testing mechanism. Gartner has predicted that by 2025, 60% of organizations will embrace a zero-trust security strategy³⁴.

³⁴<https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network>

8. **Supply Chain Security:** While device manufacturers make efforts to follow the best practices internally, it is equally important to manage the risk introduced by external (component) suppliers, vendors etc. This is a complex topic, as it requires tracing the origin of each hardware component from source until to destination. Compromised supply chain can jeopardise the whole ecosystem. A good example is presence of counterfeit components in the supply chain, which can be highly detrimental to the reliability, and security of the product. While most of the counterfeit products are of poor-quality/ refurbished products, some may be especially engineered with backdoors and exploits that are extremely hard to detect. Observing the criticality and security challenges, the National Policy of Electronics (NPE) 2019 defines it under Trusted Electronic value chain (refer section 3.5).

9. **Software Bill of Material (SBoM):** A Software Bill of Materials (SBoM) is a complete, formally structured list of components, libraries, and modules that are required to build (i.e., compile and link) a given piece of software and the supply chain relationships between them³⁵. When flaws or vulnerabilities are discovered in any of the components, SBoMs could be used to quickly identify software systems that are affected by the vulnerable component. SBoMs are also used to assess the usage of a software, and to understand the risk introduced by the vulnerable component. The ability to identify vulnerabilities allows software suppliers to produce patches or provide other remediation options; allows consumers to detect threats and apply mitigations independently of the software supplier.

Security cannot be an afterthought; it must be taken care from the design phase itself. Therefore, it is important that the manufacturers should follow the standards laid down by various standardisation / statutory bodies and industry best practices.

To ensure the safety and security of the IoT devices, it is required to test in the labs based on Essential Requirements (ERs) under Mandatory testing and Certification of Telecom equipment (MTCTE) regime of Government of India (details in section 3.3). ERs are having testing specifications related to Electromagnetic Compatibility (EMC), Safety, communication interfaces, Internet Protocol (IP), Specific Absorption Rate (SAR) and Security. Security specifications being prepared in ITSAR (Indian Telecom Security Assurance Requirements) are the part of the ERs.

Any of the devices in the network (tested under MTCTE or not tested/ not covered in MTCTE) may become vulnerable.

To develop a secured IoT eco system as well as to address the vulnerabilities related issues, work being carried out at national / international level has been studied and listed in the forthcoming sections.

³⁵https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_faq_-_april_15_draft.pdf

3. Existing policies, standards and guidelines related to M2M / IoT security in India

3.1. DoT policies in M2M/ IoT domain

DoT has released a series of policy documents/ guidelines/ circulars for the proliferation of M2M / IoT domain, as listed below:

Policy Documents:

- *National Digital Communication Policy*³⁶ released in 2018
- *National Telecom M2M Roadmap*³⁷ released in 2015

Guidelines and Circulars:

- *Guidelines for Registration Process of M2M Service Providers- M2MSP and WPAN/WLAN Connectivity Providers for M2M Services*³⁸ released in Feb 2022.
- *Guidelines for grant of unified license (Virtual Network Operators)*³⁹ released in January 2022.

3.1.1. National Digital Communication Policy (NDCP) 2018

NDCP 2018 was released by Department of Telecommunications in 2018. It covers many points related to IoT, Artificial Intelligence and 5G.

Extract related to IoT, 5G and other emerging technologies in NDCP is as given below:

1. **Propel India:** Enabling Next Generation Technologies and Services through Investments, Innovation, Indigenous Manufacturing and IPR Generation

2022 Goals:

- a. Expand IoT ecosystem to 5 billion connected devices by 2022.
- b. Creation of innovation led Start-ups in Digital Communications sector.
- c. Train/ Re-skill 1 million manpower for building New Age Skills.

³⁶<https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf>

³⁷<https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf>

³⁸<https://dot.gov.in/latestupdates/guidelines-registration-process-m2m-service-providers-m2msp-and-wpanwlan-connectivity>

³⁹https://dot.gov.in/sites/default/files/UL%20VNO%20guidelines%20with%20M2M%20without%20INSAT%20MSS%20R%20dated%2017012022_1.pdf

2. Accelerating Industry 4.0

- a. Create a roadmap for transition to Industry 4.0 by 2020 by closely working with sector specific Industry Councils.
- b. Establish a multi-stakeholder led collaborative mechanism for coordinating transition to Industry 4.0.
- c. *Developing market for IoT/ M2M connectivity services in sectors including Agriculture, Smart Cities, Intelligent Transport Networks, Multimodal Logistics, Smart Electricity Meter, Consumer Durables etc. Incorporating international best practices.*

3. Ensuring a holistic and harmonized approach for harnessing Emerging Technologies

- a. Creating a roadmap for emerging technologies and its use in the communications sector, such as *5G, Artificial Intelligence, Robotics, Internet of Things, Cloud Computing and M2M.*
- b. Synergising deployment and adoption of new and emerging technologies by:
 - i. Simplifying licensing and regulatory framework whilst ensuring appropriate ***security framework for IoT/ M2M/ future services and network elements incorporating international best practices.***
 - ii. Earmarking adequate licensed and unlicensed spectrum for IoT/ M2M services.
 - iii. Encourage use of Open APIs for emerging technologies.
 - iv. Ensuring the Transition to Ipv6 for all existing communications systems, equipment, networks and devices.
 - v. Enabling Hi-speed internet, Internet of Things and M2M for rollout of 5G technologies and services.
 - Implementing an action plan for rollout of 5G applications and services.
 - Enhancing the backhaul capacity to support the development of next-generation networks like 5G.
 - Ensuring availability of spectrum for 5G in < 1 GHz, 1-6 GHz and > 6 GHz bands.
 - Reviewing industry practices with respect to traffic prioritization to provide 5G enabled applications and services.
 - ***Developing framework for accelerated deployment of M2M services while safeguarding security and interception for M2M devices.***
 - Defining policy for EMF radiation for M2M devices, with accompanying institutional framework to coordinate

government-funded and India-specific research in this regard.

4. Ensuring adequate numbering resources, by:

Allocating 13-digit numbers for all M2M mobile connections.

5. Recognizing Digital Communications as the core of Smart Cities by:

- a. Developing, in collaboration with Ministry of Urban Development, a Common Service Framework and Standards for Smart Cities.
- b. Facilitating and supporting deployment of innovative solutions in identified Smart Cities.

6. Promoting research & development in Digital Communication Technologies by:

- a. Creating a framework for testing and certification of new products and services.

3.2. M2M/ IoT standardisation in TEC

TEC has been working in M2M/ IoT domain since 2014, and created a framework for finalizing specifications in sync with global bodies. To study the M2M/ IoT domain, TEC formed multi-stakeholders working groups time to time and released eighteen Technical Reports (TRs) with the outcome intended to be used in policy / standards. These Technical Reports cover diverse verticals namely Power Sector, Automotive (Intelligent Transport system), Remote Health Management, Safety & Surveillance, Smart Homes, Smart Cities, Smart Village & Agriculture; and also, in the horizontal layer such as M2M Gateway & Architecture, Communication Technologies and Security aspects in M2M/ IoT domain. Several recommendations of these technical reports are the part of policies/ standards and others are under discussion. All the Technical Reports are available on TEC website⁴⁰. TEC adopted oneM2M Release 2 and Release 3 specifications (transposed by TSDSI) as National Standards (details in section 3.2.4).

All the work done by TEC in M2M/ IoT domain is available in brief in the report on “TEC / Initiatives in M2M / IoT domain- An overview”. The report is available on TEC website⁴¹.

It is worth mentioning that the International Telecommunication Union (ITU) has posted the following five TEC Technical Reports on its website⁴² in IoT sections (2022 and 2021), recognizing as insightful technical resource for the benefit of global community :

- (i) Framework of National Trust Centre for M2M/IoT Devices and Applications
- (ii) IoT/ ICT Standards for Smart Cities

⁴⁰ <https://www.tec.gov.in/M2M-IoT-technical-reports>

⁴¹ https://www.tec.gov.in/pdf/M2M/Report_TEC%20initiatives%20in%20M2M%20IoT%20domain.pdf

⁴² <https://www.itu.int/cities/dt-resource-hub/iot/>

- (iii) Emerging Communication Technologies & Use Cases in IoT Domain
- (iv) Code of Practice for Securing Consumer Internet of Things (IoT)
- (v) IoT/ ICT Enablement in Smart Village and Agriculture

Out of eighteen, three Technical Reports (TRs) as listed below are related to IoT Security:

1. ***Framework of National Trust Centre for M2M/IoT Devices and Applications***, released in March 2022.
2. ***Code of practice for Securing Consumer IoT***, released in August 2021.
3. ***Recommendations for M2M/ IoT Security***, released in 2019.

Technical Reports mentioned at point no. 1 & 2 above are with reference to the TRAI work items mentioned in executive summary of this document. Above documents are being summarized below:

3.2.1. TEC TR - Framework of National Trust Centre (NTC) for M2M / IoT devices and Applications

As the certification of the M2M /IoT devices under MTCTE (refer section 3.3) regime has just started therefore IoT/ Smart City ecosystem will be having certified as well as non-certified devices in the network. Vulnerabilities /security related issues may arise in any type of IoT devices working in the network. Technical report on *the Framework of National trust Centre for M2M / IoT devices and Applications* visualises its implementation in a phased manner for managing/ addressing the vulnerability related issues of IoT devices reported by IoT/ Smart city platforms working in the network. NTC project is under implementation.

3.2.2. TEC TR - Code of practice for Securing Consumer IoT

It provides guidance to the related stakeholders in provisioning of secured consumer IoT devices and help in reducing vulnerabilities. It has thirteen guidelines as listed below and, mainly applies to IoT Device Manufacturers, IoT service providers/ System integrators and Mobile application developers:

1. No universal default passwords
2. Implement a means to manage reports of vulnerabilities
3. Keep software updated
4. Securely store sensitive security parameters
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is secure
9. Make systems resilient to outages
10. Examine system telemetry data
11. Make it easy for users to delete user data
12. Make installation and maintenance of devices easy
13. Validate input data

This technical report is based on the guidelines available in ETSI TS 103 645.

DoT has issued the Office Memorandum (O.M.) 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 O.M. in March 2023 to M2M service providers to follow the first three guidelines of this technical report.

This TEC TR has been mentioned in the IoTSF document ***Contemporary use of Vulnerability disclosure in IoT***⁴³ released in Nov 2021. In this document IoTSF has given a number of recommendations for managing the vulnerability related issues (details in section 4.7.1).

3.2.3. TEC TR - Recommendations for M2M/ IoT Security

This document⁴⁴ has defined various IoT architectures including oneM2M, Security challenges, M2M/ IoT End point security based on assurance levels and also classified the use cases based on the risk associated with the application such as criticality of the application, quality of service needed and sensitivity of the data e.g. Mission Critical, High QoS, Sensitive Information [CQS]; Mission Critical, High QoS, Non-Sensitive Information [CQN] etc.

Assurance levels and the classification of devices have been referred in detail in section-6 for mapping the different classification/ labelling schemes.

3.2.4. Adoption of oneM2M specifications in India

TEC adopted oneM2M Release 2 specifications in 2020 and oneM2M Release 3 in 2022 as National Standards, its TS-0003 is related to IoT security solutions.

These TEC National Standards have been referred as normative and informative references by BIS in its standard on IoT reference architecture IoT RA IS 18004 (Part 1): 2021. MoHUA has referred BIS IoT Reference Architecture in the ICC/ ICT Model RFP2.0 (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>).

ITU-T SG-20 has adopted oneM2M Release 2 specifications and published as ITU standards.

⁴³<https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf>

⁴⁴<https://tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20IoT%20M2M%20Security.pdf>

3.2.5. Mandatory Testing and Certification of Telecom Equipment (MTCTE)

Department of Telecommunications, Ministry of Communications has notified “Indian Telegraph (Amendment) Rules” in Gazette of India vide G.S.R. 1131(E) PART XI" on 5th September 2017 which prescribes for Mandatory Testing and Certification of Telecommunication Equipment. Any telegraph which is used or capable of being used with any telegraph established, maintained, or worked under the licence granted by the Central Government in accordance with the provisions of section 4 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act), shall have to undergo prior mandatory testing and certification in respect of parameters as determined by the telegraph authority from time to time.

Telecommunication Engineering Centre, New Delhi, under Department of Telecommunications (DoT), which, inter alia, is the Telegraph Authority for the purpose of Testing and Certification. The testing is to be carried out by TEC Accredited labs and based upon their test reports, certificate shall be issued by TEC.

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 Essential requirements (ERs) for testing of telecom equipment as well as some IoT devices (including variants) have been prepared with the related stakeholders’ consultations. All the ERs and ITSARs are available on TEC MTCTE portal⁴⁵.

3.2.6. International participation

DoT is the state member of ITU and TEC has been mandated to participate in ITU-T activities. For IoT and Smart cities related standardisation work, TEC participates in ITU-T SG-20, ITU-T SG-17, ITU-R WP 5D, ITU-T FG AI4A, ISO/ IEC JTC1 SC41, APT, AWG, ETSI Security week, oneM2M, 3GPP, NIST webinar etc. at international level; and in BIS & TSDSI at National level. Following three recommendations of ITU-T SG 20 are having significant contributions submitted by TEC:

1. ITU-T Recommendation Y Suppl. 53 (12/2018) on *IoT use cases*.
2. ITU-T Recommendation Y Suppl. 56 (12/2019) on *Smart City use cases*.
3. ITU-T Recommendation Y. 4218 on *IoT and ICT requirements for deployment of smart services in rural community* (Approved in ITU-T SG-20 meeting, Feb 2023).

⁴⁵ <https://www.mtcte.tec.gov.in/>

3.3. National Critical Information Infrastructure Protection Center (NCIIPC)

National Critical Information Infrastructure Protection Centre (NCIIPC) an organisation of the Government of India has released Framework for Evaluating Cyber Security in Critical Information Infrastructure⁴⁶.

3.4. National Security Council Secretariat (NSCS)

The National Security Council of India is an executive government agency tasked with advising the Prime Minister's office on matters of national security and strategic interest. The National Cyber Security Coordinator (NCSC) is the Designated Authority (DA) for the determination of inclusion of a vendor as a Trusted Source, of a Telecom product as a Trusted Product and the methodology for the said inclusion.

The National Security Council aspires to be a national security institution that is responsive to changing challenges and opportunities both within and outside the country, as well as a policy advisory body that will effectively contribute to the creation of an enabling environment that will improve socioeconomic development and national governance.

It aims to protect the cyber space including critical information infrastructure from attack, damage, misuse and economic espionage.

In a move towards ensuring National security, The Department of Telecommunications (DoT), Government of India has amended the telecom licenses to mandate the use of equipment only from "trusted sources" from June 15, 2021⁴⁷. DoT in its press release has mentioned that "The government through the designated authority will have the right to impose conditions for procurement of telecommunication equipment on grounds of defence of India or matters directly or indirectly related thereto for national security". It further quotes "With effect from 15th June 2021, the licensee shall only connect trusted products in its network, and also seek permission from designated authority for upgradation of existing network utilising the telecommunication equipment not designated as trusted products".

3.5. Ministry of Electronics & Information Technology (MeitY)

MeitY released National Cyber Security Policy -2013 (NCSP-2013) with mission to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities, and minimize damage cyber incidents through combination of institutional structures, people, processes, technology and cooperation. Objective of NCSP-2013 includes to create an assurance framework for design and security policies and for promotion and enabling actions for compliance to global security standards and best practice by the way conformity assessment (product, process, technology, and people).

As mentioned in section 3.5.1(Trusted Electronic Value Chain) of the gazette notification No.26(1)/2019-IPHW dated 25.02.2019, of National Policy on Electronic (NPE⁴⁸) 2019, trusted

⁴⁶https://nciipc.gov.in/documents/Evaluating_Cyber_Security_Framework.pdf

⁴⁷<https://dot.gov.in/sites/default/files/2021%2003%2031%20UL%20Proc%20AS-I.pdf?download=1>

⁴⁸https://www.meity.gov.in/writereaddata/files/eGazette_Notification_NPE%202019_dated%2025022019.pdf

device, software (Boot loader, Operating System, Application), and even the active programming code that exists in supply chain components, should be the focus to securitise the devices.

3.5.1. Standardisation Testing and Quality Certification (STQC)

STQC Directorate, an attached office of the Ministry of Electronics and Information Technology, provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres. The services include Testing, Calibration, IT & e-Governance, Training and Certification having National / International accreditation and recognitions in the area of testing and calibration.

In the area of IT & e-Governance, STQC provides Software Products/Systems and Process Assurance Services by conducting Testing, Training, Audit and Certifications. The certification is done based on following schemes:

- a) **Common Criteria:** The Indian Common Criteria Certification Scheme (IC3S), operated by STQC has the recognition by Common Criteria Recognition Arrangements (CCRA), as a Certificate Authorizing Nation (for details refer section 8.4).
- b) **Trusted Electronics Value Chain Certificate Scheme (TEVCCS):** This scheme is to promote Trusted Electronics Value Chain initiatives for ICT Products based on National Policy on Electronics 2019 (NPE 2019). This scheme will facilitate improvement of National Cyber Security profile including National Critical Information infrastructures.
- c) **IoT System Certification Scheme (IoTSCS):** This evaluation of IoT product & system covers assessment of all the sensing and embedding components (includes Sensors, Actuators etc), communication protocols, IoT Gateways, IoT cloud, End-user devices and user interface etc. Assessment of IoT devices covers basically three aspects mainly physical, Communication and its application interfaces. The IoT devices scheme comprises of three (03) levels, with each higher level being more comprehensive in the assessment.

3.6. MoHUA guidelines on cyber security

Cyber Security Model Framework for Smart Cities has been released by MoHUA vide letter number K- 15016/61/2016-SC-I dated 20th May 2016⁴⁹. This framework has been prepared by National Security Council Secretariat, Government of India in consultation with the Industry (NASSCOM, DSCI) which defines cyber security requirements that may be necessary to be incorporated while inviting proposals/offers from the companies implementing Information Technology and applications as part of Smart Cities. MoHUA has

⁴⁹http://mohua.gov.in/pdf/58fd92b5545b85821b621a862dCyber_Securitypdf.pdf

issued advisory in November 2022 to all Smart City stakeholders regarding *Standard operating procedure for cyber security of smart city infrastructure*⁵⁰.

3.7. Bureau of Indian Standards (BIS)

BIS is having several committees for finalizing standards in various areas. Committees working in IoT and Security are listed below⁵¹:

- I. LITD 17: Information Systems Security and Privacy
- II. LITD 27: IoT and Digital Twin
- III. LITD 28: Smart Infrastructure Sectional Committee

LITD 17 is the mirror committee of ISO/IEC JTC 1/SC 27 and LITD 27 of ISO/IEC JTC1/SC41. Few important standards released by LITD 17 are as:

- IS/ISO/IEC 27007: 2017⁵² on Information security cybersecurity and privacy protection Guidelines for information security management systems auditing
- IS/ISO/IEC 27033-4: 2014 (Reaffirmed In : 2019)⁵³ on Information technology –Security techniques –Network: Security: Part 4 Securing communications between networks using Security gateways.
- IS 17737 (Part 1):2021⁵⁴ on Mobile Device Security.

BIS has also released *IoT System Reference Architecture* IS 18004 (Part 1) :2021.

3.8. Telecommunications Standards Development Society of India (TSDSI)

TSDSI 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 transposes oneM2M and 3GPP specifications time to time and submits to TEC for considering them for adoption/ ratification.

TEC, after complying with the consultation process as per the Standardisation guide, adopted TSDSI transposed oneM2M Release 2 and Release 3 specifications, as National standards⁵⁵. These national standards shall be voluntary unless made mandatory by its use, reference or adoption by regulation/ Government directive. TEC has also adopted 3GPP specifications

⁵⁰ https://smartnet.niua.org/sites/default/files/advisory_no.22.pdf

⁵¹ https://www.services.bis.gov.in:8071/php/BIS_2.0/dgdashboard/published/new_subcommitt?depid=NjY%3D

⁵² https://www.services.bis.gov.in/php/BIS_2.0/dgdashboard/published/revised_PubStn_list?depid=NjY=&depname=TEIURCA=&aspect=MA==

⁵³ https://www.services.bis.gov.in/php/BIS_2.0/dgdashboard/published/new_standards?commttid=MjM0&commttname=TEIURCAxNw%3D%3D&aspect=MA%3D%3D

⁵⁴ https://www.services.bis.gov.in/php/BIS_2.0/dgdashboard/published/new_standards?commttid=MjM0&commttname=TEIURCAxNw%3D%3D&aspect=MA%3D%3D

⁵⁵ <https://tec.gov.in/onem2m>

releases 10 to 17. It has given a way for deployment of standard based cellular services in the country⁵⁶.

4. International study on M2M/ IoT Security – Standards, Regulation & Best practices

4.1. ITU standards on IoT Security

International Telecommunication Union (ITU)'s standardization sector namely ITU-T is having the Study Group 17 (ITU-T SG 17) on **Security**⁵⁷ and Study group 20 (ITU-T SG 20) on **IoT and its applications in Smart Cities & communities**⁵⁸.

ITU-T SG-20 has released a large range of standards on IoT Devices, Gateways, Platforms, Big data, Open data, Smart data Governance, Frontier technologies (AI, ML, Blockchain), Security, Use cases, Key performance indicators (KPIs), city planning, stakeholder's engagement etc. Study Group 20 is having one question on IoT Security i.e. Q6/20: Security, Privacy and Trust.

ITU-T Study Group 17 is having following questions related to IoT security:

Q6/17: Security for telecommunication services and Internet of Things (IoT)

Q10/17: Identity management and telebiometrics architecture and mechanisms

Q11/17: Generic technologies (such as Directory, PKI, formal languages, object identifiers) to support secure applications.

Q13/17: ITS Security.

SG-17 has published a series of standards related to telecom and IoT Security.

ITU-T Recommendation X.509 (10/2019) and cor.1 (10/2021) on Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks provides Public Key Infrastructure (PKI) for device Identity, providing a scalable way to declare unique Identity and authenticating the messages of communicating parties.

The X.509 standard is the common global language for certificates used in public key infrastructure. Specifically, it defines the data structures that underpin certificates and Certificate Revocation Lists (CRLs) used across everything from internet protocols (TLS/SSL encryption) to electronic signatures to enterprise security.

In terms of certificates, the X.509 standard creates certificates using a public and private key pair. Together, this key pair can encrypt (public key) and decrypt (private key) communications as well as verify someone's identity and the integrity of communications (public key when something is signed with the private key). More details are available in

⁵⁶<https://www.tec.gov.in/standards-adoption-policy>

⁵⁷<https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx>

⁵⁸<https://www.itu.int/en/ITU-T/studygroups/2022-2024/20/Pages/default.aspx>

annexure IV. Important standards on IoT security released by ITU have been listed in Annexure-I.

4.2. ISO/IEC standards on IT/ IoT Security

International Organization for Standardization / International Electro-technical Commission (ISO/IEC) Joint technical committee 1, subcommittee 27 (ISO/IEC JTC 1/SC 27 on *Information Security, cyber security and privacy protection*⁵⁹ has published a number of standards.

ISO/IEC JTC 1/SC 27 has released standard ISO/IEC 27400: 2022 on **Cybersecurity — IoT security and privacy — Guidelines**⁶⁰ in June 2022. This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions. IoT stakeholders for the lifecycle of the IoT system may use these controls. This document in its annexures includes an example of sample risk scenario related to **CCTV/ Smart camera** deployed in network. Some of the important standards are listed in the Annexure-I.

In India, Bureau of Indian Standards (BIS) National Committee (LITD 17) is the mirror committee of ISO/IEC JTC 1/SC 27.

4.3. IEEE guidelines on IoT security

IEEE (Institute of Electrical and Electronics Engineers) has released a document on *IoT Security Best Practices*⁶¹. It has mentioned eleven best practices for securing devices and networks.

1. Make hardware tamper resistant
2. Provide for firmware updates/patches
3. Perform dynamic testing
4. Specify procedures to protect data on device disposal
5. Use strong authentication
6. Use strong encryption and secure protocols
7. Minimize device bandwidth
8. Divide networks into segments
9. Protect sensitive information
10. Encourage ethical hacking, and discourage blanket safe harbour
11. Institute an IoT Security and Privacy Certification Board

This list is not comprehensive, but it represents the kinds of activities that will result in better IoT security. Above best practices are intended to be used by IoT device manufacturers, designers, researchers, the policy makers etc.

⁵⁹<https://www.iso.org/committee/45306.html>

⁶⁰<https://www.iso.org/standard/44373.html>

⁶¹https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf

4.4. CEN-CENELEC activities on cyber-security

Three European Standards Organisations (ESOs) - CENELEC (European Committee for Electrotechnical Standardization), ETSI (European telecommunications Standards Institute) and CEN (European Committee for Standardisation on other technical areas) forms the European system for technical standardization. Standards developed and harmonised by these agencies are regularly adopted in many countries outside Europe which follow European technical standards. Cybersecurity has been identified as one of the standardization priorities, since cyber-threats impact a multitude of sectors. Cybersecurity and data protection are rapidly growing and changing technical and application domains. The threats and requirements are increasing dramatically with the progress of digitalization and the rising number of critical assets digitalized and accessible online. Therefore, protection is expected from citizens but also industry and even governments

1. **CEN/CENELEC JTC 13 'Cybersecurity and data protection'** is the CEN and CENELEC horizontal technical committee that addresses these needs. Its primary objective is to transport relevant international standards (especially from ISO/IEC JTC 1 SC 27) as European Standards (ENs) in the Information Technology (IT) domain. It also develops 'home-grown' ENs, where gaps exist, in support to EU regulations (RED, eIDAS, GDPR, NIS, etc.). These two streams of activities aim at creating a strategic portfolio of standards in Europe, which fits the European needs. CEN-CLC/JTC 13 works closely with **ENISA** (The European Union Agency for Cybersecurity) in the context of the European certification schemes, and with the European Commission, in the frame of the cybersecurity-related standardization request under the Radio Equipment Directive (RED).
2. **CLC/TC 65X 'Industrial-process measurement, control and automation'** is another main provider of cybersecurity-related standards in the Operational Technology (OT) domain. It prepares standards for systems and elements used for industrial process measurement, control and automation. It has created the EN IEC 62443 series of standards for Operational Technology (OT) found in industrial and critical infrastructures, including but not restricted to power utilities, water managements systems, healthcare and transport systems.
3. **CEN/TC 114 'Safety of machinery'** produces standards and other documents on general principles for the safety of machinery, including terminology and methodology has developed a TR on the impact of cybersecurity for machines safety: ISO/TR 22100-4:2020 Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects (ISO/TR 22100-4:2018).

4.5. ENISA -Baseline Security Recommendations for IoT

ENISA (European Union Agency for Cybersecurity) is the European Union's agency dedicated to achieving a high common level of cybersecurity across Europe. It has released a number of documents related to Cyber Security. ENISA in its document released in 2017 on **Baseline**

Security Recommendations for IoT⁶² reviewed several existing IoT architectures and based on them, defined a common architecture for IoT security as depicted in the figure-9. The main IoT architectures reviewed are listed below:

- AIOTI High Level Architecture functional model
- FP7-ICT – IoT-A Architectural reference model
- NIST special publication 800-183, Network of Things
- ITU-T IoT reference model
- ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)
- ISACA Conceptual IoT Architecture
- oneM2M Architecture Model
- IEEE P2413 - Standard for an Architectural Framework

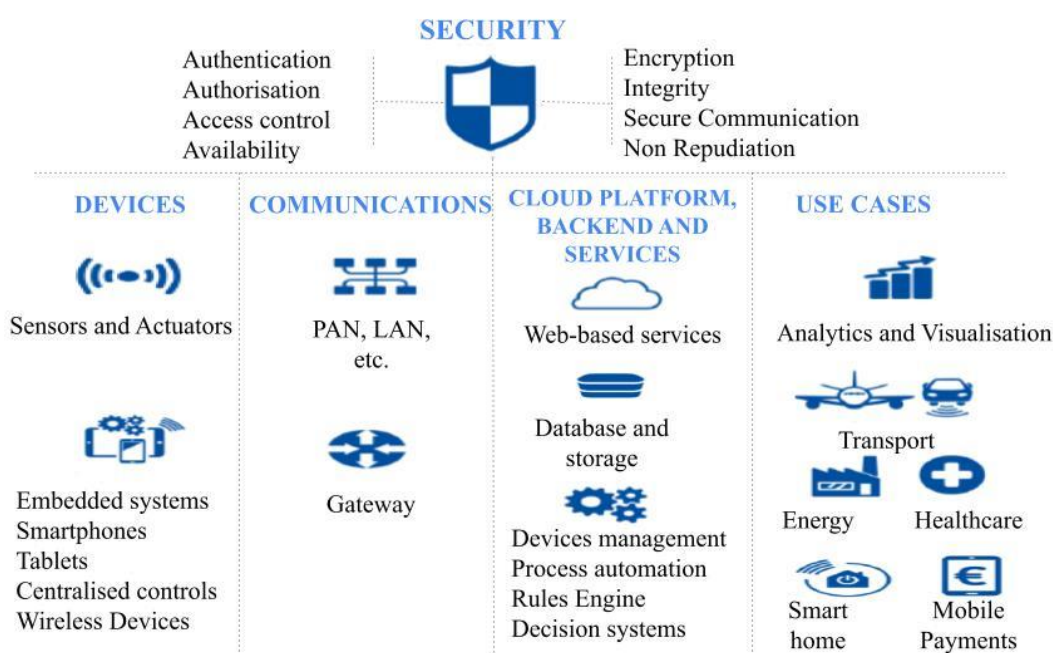


Figure 9: Summary requirements for IoT Security⁶³

ENISA's objective was to utilise this high-level reference model to define the assets for IoT security and to assist stakeholders in consistently applying methodology in identifying threats and attacks.

ENISA in its report *'Good Practices for Security of IoT'*, released in 2019, highlighted the 'Security by design for IoT'. The report focuses on software development guidelines, a key aspect for achieving security by design. The report elaborates and delves into this notion by giving specifics on how to securely collect requirements, design, develop, maintain, and even dispose of IoT systems and services⁶⁴.

⁶²<https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

⁶³ENISA -Baseline Security Recommendations for IoT, November 2017

⁶⁴ <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1/@/download/fullReport>

ENISA document on *Coordinated Vulnerability Disclosure Policies in the EU*⁶⁵, released in 2020 covers the information about coordinated vulnerability disclosure (CVD) policies of 27 countries of European Union and mentioned the key findings as well as the recommendations such as *active participation of security researchers in CVD programme and needs to be promoted by the member countries*.

4.6. ETSI Standards on consumer IoT Security

ETSI (European Telecommunications Standards Institute) Technical Committee on Cybersecurity (ETSI TC CYBER) released cyber security standard for consumer IoT devices in June 2020 addressing the consumer IoT security.

4.6.1. ETSI TS 103 645 - Cyber Security for Consumer Internet of Things

This standard specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services. This standard⁶⁶ is said to be the first globally applicable standard on consumer IoT security. A non-exhaustive list of examples includes:

- connected children's toys and baby monitors;
- connected safety-relevant products such as smoke detectors and door locks;
- smart cameras, TVs and speakers;
- wearable health trackers;
- connected home automation and alarm systems;
- connected appliances (e.g. washing machines, fridges); and
- smart home assistants.

ETSI TS 103 645 is having the following basic requirements for consumer IoT security:

1. No universal default passwords
2. Implement a means to manage reports of vulnerabilities
3. Keep software updated
4. Securely store sensitive security parameters
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is secure
9. Make systems resilient to outages
10. Examine system telemetry data
11. Make it easy for users to delete user data
12. Make installation and maintenance of devices easy
13. Validate input data

⁶⁵<https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu>

⁶⁶https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

ETSI TS 103 645 has been adopted by EU as ETSI EN 303 645 as a Baseline requirements for cyber security of consumer Internet of Things.

ETSI TC CYBER has also released **Assessment Specifications**⁶⁷ ETSI TS 103 701 in August 2021 to specify conformance assessments of baseline requirements for assessing consumer IoT products against the provisions of ETSI EN 303 645. It sets out mandatory and recommended assessments as well as conditions and complements of ETSI TS 103 645/ETSI EN 303 645 by defining test cases and assessment criteria for each provision, intended to be used by testing labs and certifying bodies that provide assurance on the security of relevant products, as well as manufacturers that wish to carry out a self-assessment.

Another document named as **Implementation guide**⁶⁸ (ETSI TR 103 621) released in March 2022, provides easy-to-use guidance to help manufacturers and other stakeholders to meet the provisions defined for Consumer IoT devices in ETSI EN 303 645. It includes a non-exhaustive set of example implementations that meet the provisions in the EN.

ETSI EN 303 645 provides a security baseline requirement that spans a variety of consumer IoT devices, but sometimes additional sector-specific requirements need to be stipulated to standardise device security. TC CYBER supports new work items to create sector-specific standards (adding provisions to ETSI EN 303 645 or TS 103 701) to create a new vertical standard for a sector. For this purpose, TC CYBER created templates providing a structured way to extend ETSI EN 303 645 and ETSI TS 103 701 into a vertical domain, with adapted or new provisions in cyber security and data protection and their testing. Even if it is not an IoT device, the generic character of EN 303 645 made it appropriate as a baseline for a TS on Home Gateway Security (TS 103 848). Currently, TC CYBER is working on other verticals like smart door locks and voice-controlled devices, based on ETSI EN 303 645.

4.6.2. International alignment and adoption

ETSI EN 303 645 is a cohesive standard that presents an achievable, single target for manufacturers and IoT stakeholders to attain. Many organizations have already based their products and certification schemes around this standard. Following figure⁶⁹ illustrates how one standard can support many assurance schemes and provide flexibility in certification.

⁶⁷https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

⁶⁸https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.01.01_60/tr_103621v010101p.pdf

⁶⁹https://www.etsi.org/images/files/Magazine/ETSI_Enjoy_MAG_2021_N02_April.pdf



Figure 10 : International Alignments

Some of the organisations which have adopted the ETSI EN 303 645 standard for creating guideline and testing & certification are listed below:

- Cybersecurity Labelling Scheme, CSA Singapore
- Consumer IoT Labelling and certification Scheme, Finland
- PSA Certified
- The Global Certification Forum
- TÜV Sud testing
- TÜV Rheinland worldwide testing and certification
- VDE institute testing
- SESIP by Global Platform
- SGS IoT Testing and Conformity Assessment Program
- DEKRA security evaluations
- UL's IoT security Rating assesment, verification and labelling solution
- SafesShark and BSI IoT cyber security assessments, testing and certification
- Bureau Veritas Type Certification for IoT Devices
- ioXt's development of an assurance profile
- Eurosmart, KIWA, Secura, Nemko, ACCS, IASME etc.

4.6.3. ETSI TS 103 848 - Cyber Security for Home Gateways

Based on the provisions available in the standard ETSI EN 303 645, technical specifications on *Cyber security for Home Gateways - Security Requirements as vertical from Consumer Internet of Things*⁷⁰ was released by ETSI in March 2022 as TS 103 848. This technical specification will secure physical devices between the in-home network and the public network, as well as the traffic between these networks. The Home Gateway is connected, on one side, to the Internet service provider's network and, on the other side, to the user's Local Area Network (LAN). On the Internet service provider's network side, home gateway is exposed to other risks and attacks from a consumer IoT device.

4.6.4. ETSI initiatives in Quantum - Safe Cryptography

The introduction of quantum computing brought with it the promise of enhanced security to counter the looming threat to global information infrastructure. The basis of public key cryptography, which is widely employed on the internet, rests on mathematical problems that are deemed difficult to solve with existing computational power. However, the advent of quantum computers poses a significant threat to widely-used cryptographic schemes such as RSA and Elliptic Curve Cryptography. This threat has the potential to compromise the security of existing systems, impacting any industry that relies on secure information. The standardization of cryptographic algorithms is a significant challenge that is currently underway in various standardization bodies worldwide.

During the key distillation phase of the quantum key distribution (QKD) protocol, incorporating a quantum-safe public key algorithm along with X.509 certificates could potentially be used to authenticate the necessary service channel in QKD⁷¹.

4.7. IoT Security Foundation

IoT security Foundation (IoTSF) has released a series of documents on best practices, assurance, Vulnerabilities related to IoT Security. Few important documents have been mentioned below⁷² :

4.7.1. The Contemporary Use of Vulnerability Disclosure in IoT (Report 4, Nov 2021)

This document mentions that vulnerability disclosure policy is a vendor's statement available in the form of a public document on its webpage, as to how they will handle any vulnerability report passed to them. Reporting a product security issue should be made simple so that a vendor can get to work on applying a fix as soon as possible. Vulnerability disclosure policies

⁷⁰https://www.etsi.org/deliver/etsi_ts/103800_103899/103848/01.01.01_60/ts_103848v010101p.pdf

⁷¹<https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>

⁷²<https://www.iotsecurityfoundation.org/best-practice-guidelines/>

are expected to cover all stages of the process from advertising the correct point of contact, through to the timeline for fixing any issues and recognition for any bugs discovered.

Sections in this document⁷³ on “Research Analysis and Development”, “Recommendations from IoTSF” and “Conclusions” available on page no’s 9, 18 and 19 respectively seem to be quite important from the point of view of vulnerability disclosure and security. Important points of the recommendations are:

- **Government should mandate Vulnerability reporting as part of regulatory requirement.**
- **Technology, product or services provider: create and maintain a Vulnerability disclosure programme (VDP).**
- **Security Researchers: keep finding vulnerabilities and report them.**
- **Customers and Users: check whether a company has a Policy before purchase.**

4.7.2. Consumer IoT Security Quick Guides: No universal default password

This document⁷⁴ released in 2020 has analysed the importance of *no default password* as the users are unlikely to change a password unless forced to, thus increasing risks associated with universal passwords. It is important to mention that:

- Universal passwords can be a vulnerability for IoT devices and their users.
- Poorly managed/used passwords put users, personal data, and devices at risk.
- Attackers can co-opt devices with weak passwords, putting networks and connected things at risk.
- Failure to comply with existing standards or regulation can result in reputational and financial damage.

This Quick Guides build upon the ETSI EN 303 645 specification on consumer IoT cybersecurity.

This document has mentioned that ETSI EN 303 645 is the first international standard of its kind. Based upon it, governments are publishing guidance and are preparing legislation that impact companies developing, manufacturing or providing consumer IoT products.

IoTSF has also released the Quick Guides **Vulnerability disclosure**⁷⁵, and **Software updates**⁷⁶ besides **Passwords** as detailed above, focusing on the top 3 issues identified in standards and guidance (passwords, vulnerability disclosure, and software updates).

⁷³ <https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf>

⁷⁴ https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Passwords-QG_FINAL.pdf

⁷⁵ https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Vulnerability-QG_FINAL.pdf

⁷⁶ https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Updates-QG_FINAL.pdf

4.7.3. IoT Security Assurance Framework (Release 3.0, November 2021)

*IoT Security Assurance Framework*⁷⁷ leads its user through a structured process of questioning and evidence gathering. This ensures suitable security mechanisms and practices are implemented. The Framework is intended to help all companies make high-quality, informed security choices by guiding them through a comprehensive requirement checklist and evidence gathering process. The evidence gathered during the process can be used to declare conformance with best practice to customers and other stakeholders.

This document is the updated version of *IoT Security Compliance Framework (Version 2.1, 2020)*. Name of the document has been changed to “Assurance framework” from “Compliance Framework”. Device classification based on assurance levels as available in this document has been referred in section 6.

4.7.4. Vulnerability Disclosure Best Practice Guidelines (Release 2.0, Sept 2021)

This document⁷⁸ provides best practices and guidelines for a vulnerability disclosure process for adoption by IoT solution providers, device vendors and service providers. Vulnerability disclosure policy is the Vendor’s statement as to how they will handle any vulnerability report passed to them. The Vendor should place a web page giving the contact instructions in a standard, well-known location. Section-3 of this document provides guidance to the stakeholders for the development of vulnerability disclosure process.

4.7.5. Secure Design Best Practice Guides (Release 2, December 2019)

The IoTSF Secure Design Best Practice Guides⁷⁹ are explicitly focused at companies which are adding connectivity making IoT products. They are intended to be pragmatic and easily consumable for those with limited security knowledge and cover the most common issues. This document provides awareness and advice on the most salient elements namely *Physical security, Device secure boot, Secure operating system, Application security, Credential management, Encryption, Network connections, securing software updates, Logging, Software update policy, assessing a secure boot process, Software image & update signing and Side channel attacks that affect product, service, and user security.*

4.8. National Institute of Standards and Technology (NIST)

NIST’s Cybersecurity for the Internet of Things (IoT) program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. The following documents encompass the range of guidance for IoT cybersecurity, with the goal of ensuring

⁷⁷<https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf>

⁷⁸<https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf>

⁷⁹https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf

IoT devices are integrated into the security and privacy controls of US federal information systems⁸⁰. Some of the standards released by NIST are given below.

4.8.1. Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53)

This document provides guidance for a proactive and systemic approach for developing comprehensive safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices. The objective is to manage mission, business, and system risks for organizations, making the systems more penetration-resistant to cyber-attacks; limiting the damage from those attacks when they occur; making the systems cyber-resilient and survivable; and protecting the security and privacy of information.

4.8.2. Consideration for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228)

NISTIR 8228⁸¹ released in June 2019, provides guidelines to help organizations better understand and manage the cybersecurity and privacy risks associated with individual Internet of Things (IoT) devices throughout the devices' lifecycles. This document is intended to be useful for IoT device manufacturers and integrators for understanding concerns regarding managing cybersecurity and privacy risks for IoT devices.

4.8.3. IoT Device Cybersecurity Guidance for the Federal Government (SP 800-213)

SP 800-213⁸² is meant for providing the IoT Device Cybersecurity Guidance for the Federal (USA) Government. This document explains the role of IoT devices as elements of federal systems and provides guidance for addressing the unique risks such devices can present; help organizations, how an IoT device they plan to acquire can integrate into a system.

It also provides guidelines for the organizations to establish IoT device cyber security requirements, device security controls and expectations from the manufacturer and / or third parties when integrating such systems.

4.8.4. Foundational Cybersecurity Activities for IoT Devices Manufacturers (NISTIR 8259)

This document⁸³ describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. These foundational cybersecurity activities can help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised devices.

⁸⁰<https://www.nist.gov/topics/cybersecurity>

⁸¹<https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf>

⁸² <https://csrc.nist.gov/publications/detail/sp/800-213/final>

⁸³<https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf>

4.8.5. IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A, May 2020)

This document⁸⁴ defines an Internet of Things (IoT) device cybersecurity capability core baseline, which is a set of device capabilities generally required to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems. These cyber security capabilities for IoT devices are namely *Device Identification, Device Configuration, Data Protection Logical Access to Interfaces, Software Update and Cybersecurity State Awareness*. This document provides organizations a starting point in identifying the device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire.

4.8.6. Profile of the IoT Core Baseline for Consumer IoT Products (NISTIR 8425, Sept 2022)

This publication⁸⁵ documents the consumer profile of NIST's Internet of Things (IoT) core baseline and identifies cybersecurity capabilities commonly needed for the consumer IoT domain (e.g. IoT products for home or personal use). IoT product capabilities have been defined in section 1.2 of this document. These capabilities may be considered as a starting point for businesses to purchase of IoT products. The consumer profile capabilities are phrased as cybersecurity outcomes that are intended to apply to the entire IoT product. This document has also mentioned the recommended consumer profile and related considerations. Table-1 (page no. 17-19) of this document on *Consumer IoT Vulnerabilities and the Relevant Capabilities from the Consumer Profile* wherein the examples of *Mirai Malware variant attacks, Unauthorized Publication of Fitness Tracker Data and Unauthorized access to home security camera data* have been given in the annexure III.

4.9. Global System for Mobile Communications – Associations (GSMA)

GSMA has released a series of documents on IoT security, few of them are as listed below⁸⁶:

4.9.1. IoT SAFE

IoT SAFE⁸⁷ (IoT SIM Applet for Secure End-to-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications. This is PKI based solution based on UICC platform provides a common mechanism to secure IoT data communications using a highly trusted SIM, rather than using proprietary and potentially less trusted hardware secure elements implemented elsewhere within the device. Some of the important features of IoT SAFE are as listed below:

- Uses the SIM as a mini 'crypto-safe' inside the device to securely establish a (D)TLS session with a corresponding application cloud/server.

⁸⁴<https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259a.pdf>

⁸⁵<https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf>

⁸⁶<https://www.gsma.com/iot/iot-security/>

⁸⁷<https://www.gsma.com/iot/iot-safe/>

- Is compatible with all SIM form factors (e.g., SIM, eSIM, iSIM).
- Provides a common API for the highly secure SIM to be used as a hardware ‘Root of Trust’ by IoT devices.

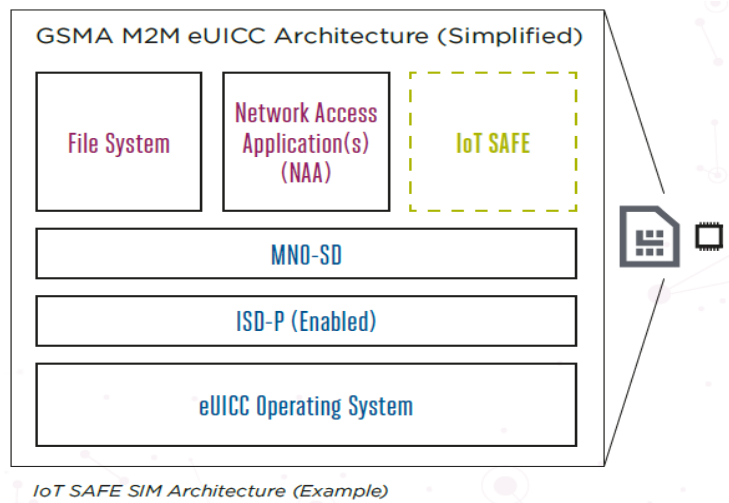


Figure 11:IoT SAFE SIM Architecture

IoT SAFE provides security services that enable:

- IoT devices to securely perform mutual (D)TLS authentication to a server using either asymmetric or symmetric security schemes
- IoT devices to compute shared secrets and keep long-term keys secret
- Provisioning and credential lifecycle management from a remote IoT security service

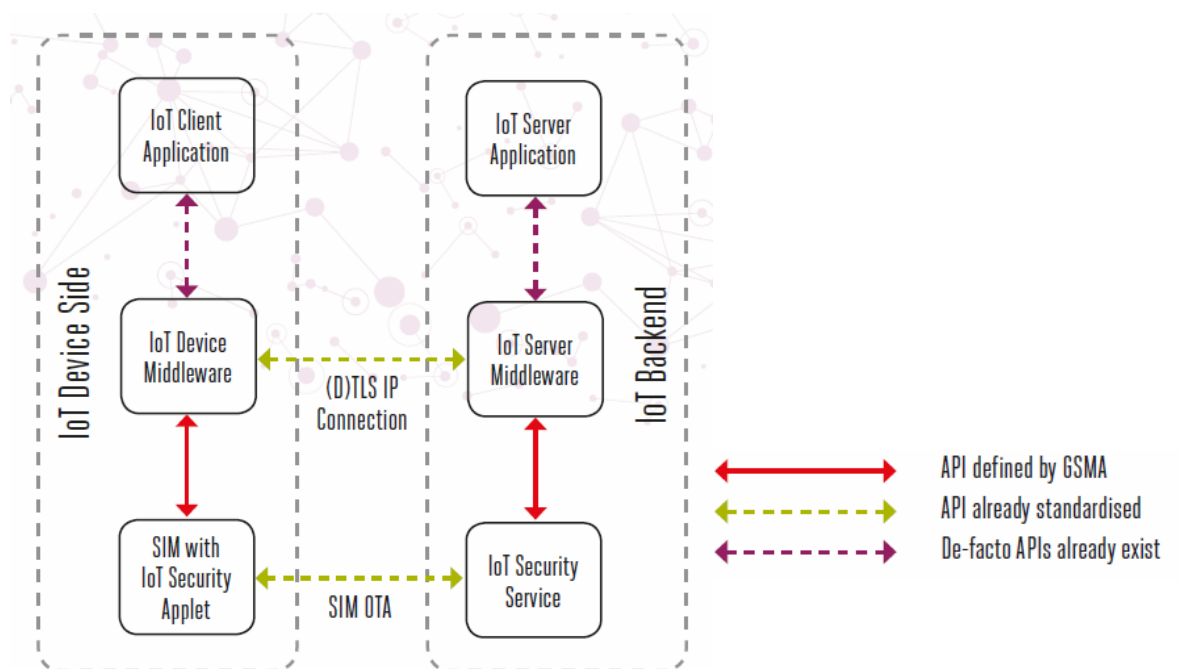


Figure 12: IoT SAFE

4.9.2. IoT Security Guidelines for Endpoint Ecosystems

This document may be used to evaluate the components of an IoT Service from the IoT Endpoint Device perspective. An Endpoint, from an IoT perspective, is a physical computing device that performs a function or task as a part of an Internet connected product or service. An Endpoint, for example, could be a wearable fitness device, an industrial control system, an automotive telematics unit or even a personal drone unit. All technologies used to drive the physical device may be evaluated for security risks. The result is a practical set of design guidelines that allow the reader to identify and remediate almost all potential risks to the IoT service⁸⁸.

4.9.3. Security Features of LTE-M and NB-IoT Networks

GSMA released this document⁸⁹ in 2019, which provides the security features as *secure by design* for LTE-M and NB-IoT to be deployed in telecom service provider network.

As mobile IoT networks use dedicated spectrum bands under the terms of the licences issued by regulators, interference from other radio technologies is kept to a minimum. Moreover, all mobile operators employ Subscriber Identity Modules (SIMs), which contain highly secure integrated circuits, to authenticate the devices accessing their networks and services. This report explains how mobile operators are supplementing these inherent capabilities with additional security features, creating significant value for their customers.

4.9.4. IoT Security Guidelines for Network Operators

This document⁹⁰ released in 2020 provides security guidelines for Network Operators who intend to provide services to IoT service providers to ensure system security and data privacy. Recommendations are based on readily available systems and technologies that are deployed today. This document also covers security features and recommendations for Mobile IoT technologies, specifically NB-IoT and LTE-M, the 3GPP industry standards for low power wide area technologies in licensed spectrum.

4.9.5. IoT Security for enterprises: make it work, make it easy

GSMA Intelligence published a survey report on *IoT security for enterprises: make it work, make it easy*⁹¹ in 2020. In this report GSMA has examined the enterprises adoption/ attitude to IoT security. It has also mentioned the enterprises current views regarding the important security features in IoT solutions, who they trust to deliver such features, and how eSIM is able to address IoT security challenges.

⁸⁸<https://www.gsma.com/iot/>

⁸⁹<https://www.gsma.com/iot/wp-content/uploads/2019/09/Security-Features-of-LTE-M-and-NB-IoT-Networks.pdf>

⁹⁰<https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.14-v2.2-GSMA-IoT-Security-Guidelines-for-Network-Operators.pdf>

⁹¹<https://www.gsma.com/iot/resources/iot-security-for-enterprises-make-it-work-make-it-easy/>

4.9.6. IoT Security Assessment Process

This document⁹² released in 2018 provides a flexible framework that addresses the diversity of the IoT market, enabling companies to build secure IoT devices and solutions as laid out in the GSMA IoT Security Guidelines, a comprehensive set of best practices promoting the secure end-to-end design, development, and deployment of IoT solutions. This document provides IoT Security Assessment process to ensure *Security by Design* and enables companies to identify and mitigate any potential security gaps in their services.

4.9.7. IoT Security guideline for IoT services ecosystem

The Service Ecosystem is a link of functionality and communication for each core facet of the overall IoT technology. All other ecosystems are dependent on the Service Ecosystem for hierarchical authentication, connectivity to users, availability, management, and other tasks critical to the day-to-day operation of IoT. The approach to accomplish the authentication, connectivity including the security, the Service Ecosystem cultivates the number of tiers to fulfil the goals of the infrastructure.

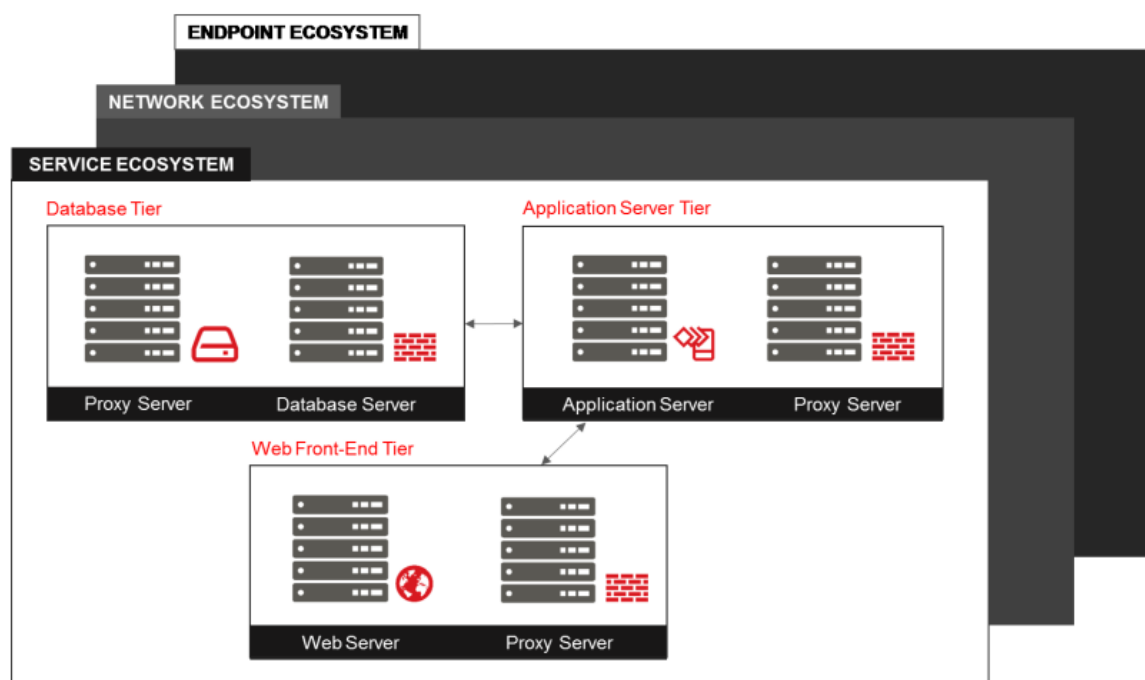


Figure 13:GSMA CLP .12 – IoT security Guidelines for service ecosystem

4.9.8. GSMA eSIM Management IT Infrastructure

Embedded SIM is evolution in SIM technology, GSMA has introduced the specification for M2M eSIM and consumer eSIM. These specifications have created the ability to remotely provision network profiles to embedded SIM (eSIM) for M2M and consumer. Remote

⁹²<https://www.gsma.com/iot/iot-security-assessment/>

provisioning infrastructure, securely provide the download/ delete/ activate/ deactivate the network profile in eSIM.

The security requirement for these Remote provisioning infrastructure shall be under secure certified area with GSMA SAS-SM accreditation including secure production of eSIM under GSMA SAS-UP accreditation. GSMA used to update and publish list for accredited organization involve in eSIM production and Remote Provisioning. Following specifications are involved in secure remote provisioning infrastructure.

- M2M eSIM specification SGP.02 for remote provisioning architecture with its entities SM-SR, SM-DP.
- Consumer eSIM specification SGP.22 remote provisioning infrastructure are SM-DP+, SM-DS.
- GSMA specification for consumer IoT SGP.31 for eSIM IoT Architecture and Requirements is for consumer IoT release in 2022 defining the IoT secure operation including IPA (IoT profile assistant).

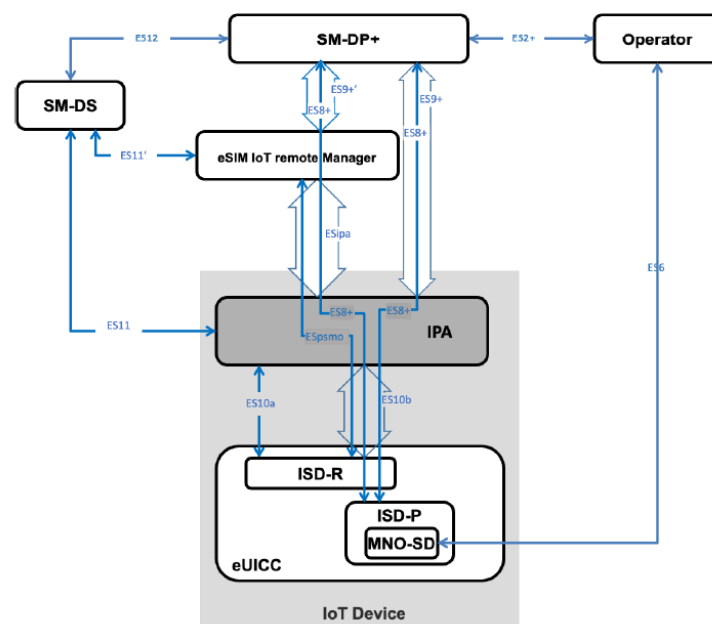


Figure 14: GSMA SGP.31 eSIM IoT architecture

Note-1: GSMA technology road map is now merging M2M and consumer eSIM and reframing the standard SGP.3x series under GSMA working group 7.

Note -2: Web links related to GSMA eSIM elements are available in Annexure V.

4.10. 3rd Generation Partnership Project (3GPP)

3GPP unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, and TTC). The 3GPP technologies from these groups are constantly evolving through Generations of commercial cellular / mobile systems. With LTE and 5G work, 3GPP has become the focal point for the vast majority of mobile systems beyond 3G.

3GPP Security working Group SA (Service and System Aspects) WG 3 ensures the availability of cryptographic algorithms which need to be part of the specifications. Within SA WG 3, the sub-working group SA WG 3-LI provides the requirements and specifications for lawful interception in 3GPP systems. SA WG 3 is currently responsible for security in the 5G System including the 3GPP enhancements for IoT and vertical industry. Some of the important 3GPP specifications related to SA WG 3 are as given below: -

- a. 5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF)
- b. Security aspects of for advanced Vehicle-to-Everything (V2X) services
- c. Study on security aspects of 5G network slicing management
- d. Study on subscriber privacy impact in 3GPP
- e. Study of privacy of identifiers over radio access
- f. Study on security aspects of Machine-Type Communications (MTC) architecture and feature enhancements
- g. Study on zero-trust security principles in mobile networks
- h. Criteria for cryptographic Algorithm design process for MILENAGE and TUAK algorithms
- i. Security aspects for inter-access mobility between non 3GPP and 3GPP access network

4.11. GlobalPlatform

GlobalPlatform⁹³ is a technical standards organization that enables the launch and management of digital services and devices for delivering end-to-end security and privacy related features.

Important provisioning includes secure component specifications; the Device Trust Architecture for accessing secure services within a device; the *IoTopia* Framework for secure launch and management of connected devices; and the SESIP Methodology for IoT device certification.

GlobalPlatform technologies are used in smart cards, smartphones, wearables and other connected devices to enable convenient and trusted digital services across verticals such as healthcare, transportation, industrial automation, smart home, government and enterprise ID, payments, telecommunication networks, utilities, smart cities etc.

GlobalPlatform works mainly in the areas of Secure by design, device lifecycle management, and autonomous, scalable and secure on boarding for IoT devices.

⁹³<https://globalplatform.org/>

4.12. Trusted Connectivity Alliances (TCA)

Trusted Connectivity Alliance⁹⁴ is a global, non-profit industry association, working to enable trust by proving security credentials of Tamper Resistant Element (TRE) in various verticals and applications such as connected, wearables, smart utilities, industry 4.0, healthcare etc. Important initiatives taken by TCA are as listed below :

- Leveraging SIM technology for IoT security.
- Ensuring eSIM interoperability for IoT use-cases.
- Interoperable profiles for in GSMA SM-DP and SM-DP+.
- Evolving and optimising 5G SIM technology to enhance 5G network services.
- Highlighting the importance of subscriber privacy in 5G.
- Promoting consistency across integrated SIM technologies.

4.13. Cyber Security Agency, Singapore

4.13.1. The IoT security landscape report

Cyber Security Agency, Singapore has identified 11 cybersecurity challenges in document on *The IoT Security landscape*⁹⁵ released in 2019. These challenges are detailed below:

Principles, Governance and Legislation

1. Cybersecurity and Privacy by Design – To identify and define foundational principles to build cybersecurity and privacy by design for IoT devices.
2. IoT Security Standards and Guidelines – To set and harmonise IoT security standards and recommendations over different application domains.
3. Evaluation and Certification – To develop globally recognised and adopted cybersecurity evaluation and certification regimes for IoT devices.
4. Future-Proof Legislation – To develop regulatory policies that are sufficiently flexible to deal with societal security needs and a constantly evolving industry.

Ecosystem Development

1. Responsible Industry Ecosystem – To transform to a responsible industry that proactively implements cybersecurity in IoT devices.
2. Supply Chain Security – To create a framework for all suppliers and service providers involved in the supply chain to adopt security principles and to deliver secure IoT components.

⁹⁴<https://trustedconnectivityalliance.org/>

⁹⁵<https://www.csa.gov.sg/news/publications/iot-security-landscape>

3. Product Lifecycle Support – To implement a framework for secure device lifecycle management and patching that is adopted by all parties involved.

Technical reference and standards

1. Device Identity and Root of Trust – To establish a chain of trust from a root of trust on resource-constrained IoT devices to develop foundationally secure devices.
2. Secure OS, Cloud and Applications – To provision security controls in device OS as well as cloud and back-end applications to guarantee security within the IoT ecosystem.
3. Secure Communications and Infrastructure – To ensure data and source integrity in the communication networks of resource-constrained IoT devices.
4. Security Monitoring and Analytics – To detect vulnerabilities, anomalies and threats in IoT deployments and to quickly respond, recover and remediate.

Figure-15 below illustrates the survey conducted by Cybersecurity agency, Singapore with the domain experts, to determine the relative importance of each challenge and thereby identify priority challenges for policymakers and industry.

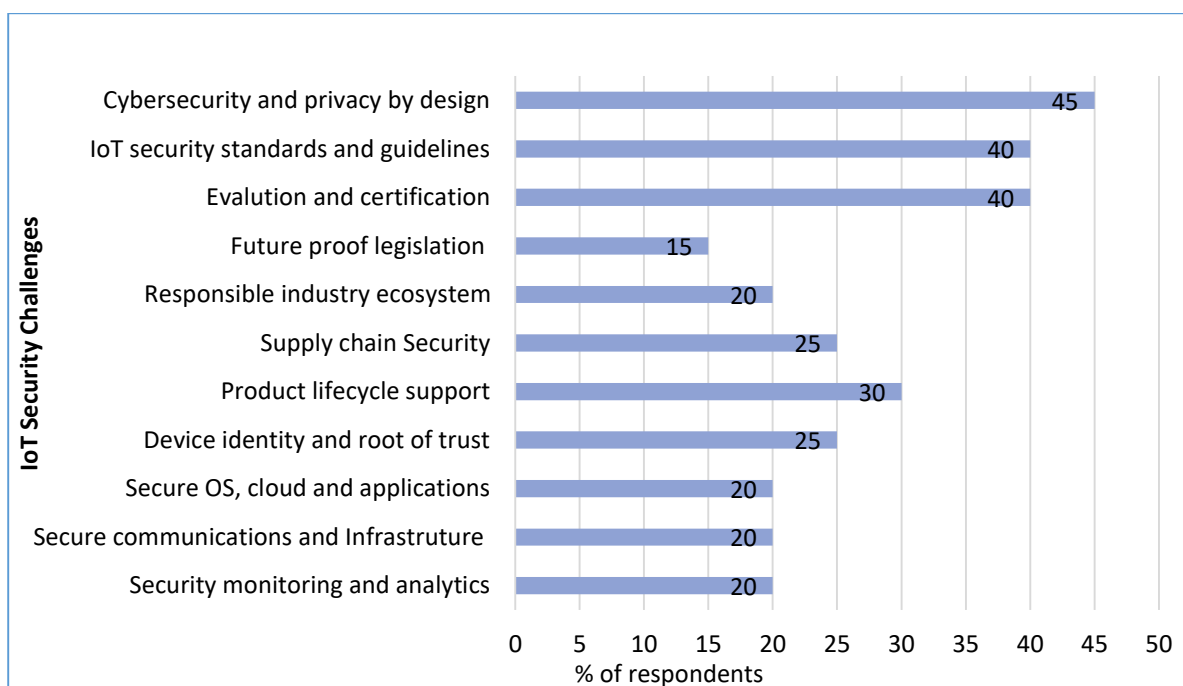


Figure 15:IoT Security challenges vs % of respondent chart⁹⁶

From this figure it appears that security is required to be built into IoT devices and ecosystems at design level. The development of effective evaluation and certification schemes built upon widely accepted security standards is increasingly seen as a cornerstone of IoT security, establishment of a secure supply chain and managed device lifecycle.

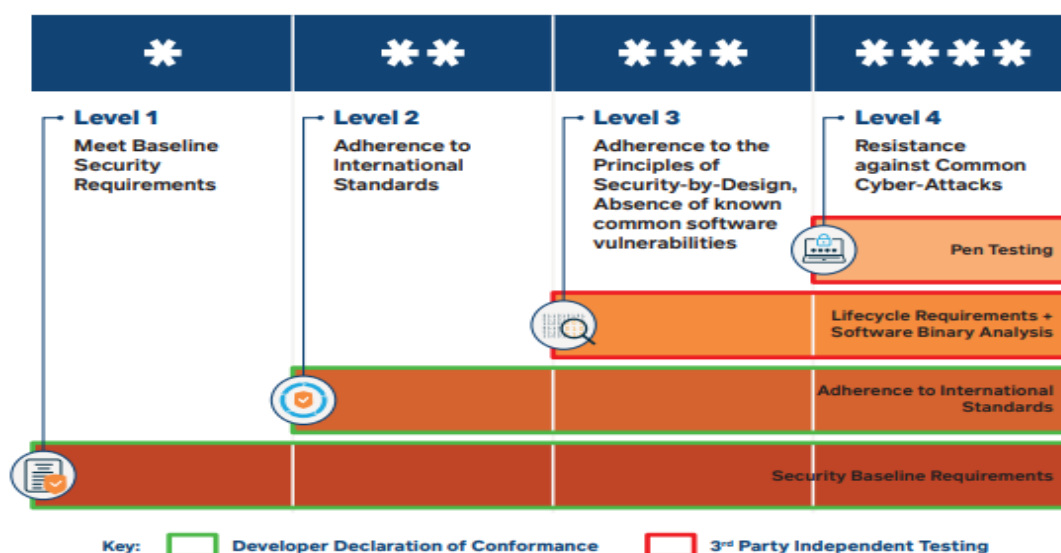
⁹⁶The IoT Security Landscape, Cyber Security Agency of Singapore

4.13.2. Cyber security Labelling Scheme, CSA Singapore

Compromised IoT devices can also be used by threat actors to form a botnet to launch Distributed Denial of Service (DDoS) attacks which could bring down Internet services. This poses cybersecurity risks such as the compromise of consumers' privacy and data as hackers generally look for the easiest systems to attack that will net the most damage and returns.

The Cyber Security Labelling Scheme (CLS)⁹⁷ for consumer IoT devices is an effort to improve the Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore cyberspace. In the scheme, smart devices will be rated according to their levels of cybersecurity provisions. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions. ***This scheme initially covered Wi-Fi routers and smart home hubs in view of their wider usage. It has been further extended to include all categories of consumer IoT devices, such as IP cameras, smart door locks, smart lights and smart printers.***

The CLS has four progressive rating levels that allows consumers to discern the level of security offered by the product and imbues security consciousness when making purchases:



[Source : Cybersecurity certification guide Singapore⁹⁸, 2021]

Figure 16: CSA labelling scheme

Level 1: Meet Baseline Security Requirements

The product meets basic security requirements such as ensuring unique default passwords and providing software updates.

⁹⁷<https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme>

⁹⁸ https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/csa-cybersecurity-certification-guide.pdf?sfvrsn=a486afd5_0

For this level, developers follow a set of baseline security requirements based on ETSI EN 303 645 in the devices by eliminating 'common mistakes' to guard against majority of attacks based on common weakness such as default password, ensuring the availability of security updates and implementing means to manage vulnerability reporting.

Level 2: Adherence to the Principles of Security-by-Design

The product has been developed using the principles of Security-by-Design⁹⁹ such as conducting threat-risk assessment, critical design review and acceptance tests, and fulfilled Level 1 requirements.

Level 3: Absence of Known Common Software Vulnerabilities

The product has undergone assessment of software binaries by approved third-party test labs and fulfilled Level 2 requirements. The software of the connected device is evaluated by a test laboratory using automated binary analysers to ensure that there is no known critical software weakness, vulnerabilities or malware.

Level 4: Resistance against common cyber attacks

The product has undergone structured penetration tests by approved third-party test labs, and fulfilled Level 3 requirements.

The connected device undergoes penetration testing by a test laboratory to provide a basic level of resistance against common cybersecurity attacks.

This labeling scheme has been referred in section 6 on Classification of IoT devices.

Mutual Recognition arrangement between (a). Singapore and Germany (b). Singapore and Finland, on Cyber Security labels of Consumer IoT products:

Singapore and **Germany** have signed a Mutual Recognition Arrangement (MRA)¹⁰⁰ to mutually recognise the cybersecurity labels issued by CSA and the Federal Office for Information Security of Germany (BSI) in 2022. Under the MRA, smart consumer products issued with Germany's IT Security Label will be recognised by CSA to have fulfilled Level 2 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 2 and above are recognised by Germany to have met their requirements.

The mutual recognition of cybersecurity labels will apply to devices intended for use by consumers such as Smart Cameras, Smart TVs, Smart Speakers, Smart Toys, Smart Garden and Household Robots, Gateways and Hubs for Home Automation, Health Trackers, Smart Lighting, Smart Plug (Smart Power Socket), and Smart Thermostats.

These products are prioritized because of their wider usage, as well as the impact that a compromise of the products could have on users.

⁹⁹ <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf>

¹⁰⁰ <https://www.csa.gov.sg/News/Press-Releases/singapore-and-germany-sign-mutual-recognition-arrangement-on-cybersecurity-labels-for-consumer-smart-products>

Singapore and **Finland** have signed a Memorandum of Understanding (MoU)¹⁰¹ to mutually recognise the Cybersecurity Labels issued by CSA and the Transport and Communications Agency of Finland (Traficom) in 2021. Under the MoU, Consumer IoT products that have met the requirements of Finland's Cybersecurity Label are recognised as having met the requirements of Level 3 of Singapore's Cybersecurity Labelling Scheme, and products with CLS Level 3 and above are recognised by Finland to have met their requirements. Level 3 and Level 4 applications for consumer connected products may be granted both Singapore's Cybersecurity Labelling Scheme label and the Finnish Cybersecurity Label at once, with a single application process. Both Singapore and Finland labels are based on ETSI EN 303 645.

4.13.3. Technical specification -Security Requirements for Residential Gateways

IMDA Singapore has released technical specification(TS) on **Security Requirements for Residential Gateways**¹⁰² in 2020. This document has defined the minimum technical security requirements for design and management of Residential IoT Gateways, for minimising the vulnerability and ensuring the protection from the security threats coming from the IoT devices and the internet. Residential gateway (IoT gateway) has also been included in the list of products which have been provided labels in view of it's wider uses (section 4.13.4). Login Credentials Management, Device Setup & Administration, Firmware Updates, Wireless Access Protection, Data Protection, Validation of Data Inputs and Vulnerabilities Reporting have been defined as the security requirements for the residential gateway.

4.13.4. Technical specification - Security Requirements to guard against Network Storms for Cellular Devices

IMDA Singapore has released technical specification on *Security Requirements to guard against Network Storms for Cellular Devices*¹⁰³ in 2022. This document has detailed the minimum technical specification for security requirements for the design and management of devices with cellular connectivity to better safeguard communication networks from security threats in the area of connection efficiency. It also sets out to minimize the vulnerability of the individual cellular devices, ensuring that these devices are better protected and secured in the areas of Access Control and Over-The-Air (OTA) updates.

4.14. UK Regulation on Consumer IoT security

UK Department for Digital, Culture, Media and Sport (DCMS) in association with National Cyber Security Centre (NCSC) released the ***Code of practice for Consumer IoT Security***¹⁰⁴ in

¹⁰¹[https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-clis#:~:text=The%20mutual%20recognition%20of%20cybersecurity,Smart%20Power%20Socket\)%2C%20and%20Smart](https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-clis#:~:text=The%20mutual%20recognition%20of%20cybersecurity,Smart%20Power%20Socket)%2C%20and%20Smart)

¹⁰²<https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Radio-Comms/IMDA-TS-RG-SEC.pdf>

¹⁰³ <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Radio-Comms/IMDA-TS-CD-SEC.pdf>

¹⁰⁴https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

2018. ETSI TS 103 645/ ETSI EN 303 645 *Cybersecurity for Consumer IoT: Baseline requirements* are having the similar principles as available in this document.

This Code of Practice sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. Implementing its thirteen guidelines will contribute to protecting consumers' privacy and safety, whilst making it easier for them to use their products securely. It will also mitigate against the threat of Distributed Denial of Service (DDoS) attacks that are launched from poorly secured IoT devices and services.

UK DCMS started the process of public consultation in 2021 for mandating the following three security requirements¹⁰⁵:

- Ban Universal default password: - It will ban manufacturers from using universal default passwords (such as "password" or "admin"), which are often pre-set in a device's factory settings and easily guessable.
- Implement a means to manage reports of vulnerabilities.
- Provide transparency on for how long, at a minimum, the product will receive security software updates.

The legislation will require smartphone and device makers to inform customers of the duration of time for which a device will receive software updates at the point of sale (PoS).

The provisions available in ETSI TS 103 645 / ETSI EN 303 645 which are inline with above mentioned three guidelines are as listed below:

5.1: No universal default passwords

5.1-1: Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

5.1-2: Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.

5.2: Implement a means to manage reports of vulnerabilities

5.2-1: The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:

- contact information for the reporting of issues; and
- information on timelines for:
 - 1) initial acknowledgement of receipt; and
 - 2) status updates until the resolution of the reported issues.

¹⁰⁵<https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation>

5.3: Keep software updated

5.3-13: The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.

UK's National Cyber Security Center (NCSC) has published advisory on the most commonly exploited vulnerabilities¹⁰⁶. NCSC has also created a **Vulnerability disclosure toolkit** as a guiding document for the stakeholders setting-up vulnerability disclosure process¹⁰⁷.

4.15. Australian regulation on IoT Security

The Australian government has released *Code of Practice: Securing the Internet of Things for Consumers*¹⁰⁸ in September, 2020. It is also having similar thirteen principles as mentioned in ETSI TS 103 645/ ETSI EN 303 645.

4.16. USA IoT Bill

In USA, state of California enacted a Bill¹⁰⁹ in 2018 for Security of Connected Devices. One of the important clause of this bill states that if a connected device is equipped with a means for authentication outside a local area network, it should meet either of the following requirements:

- I. The preprogrammed password is unique to each device manufactured.
- II. The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

On November 17, 2020, the US Senate passed the Internet of Things Cybersecurity Improvement Act (the "IoT Bill"). The IoT Bill would require the National Institute of Standards and Technology ("NIST") to develop and publish baseline standards and guidelines for how the federal government should appropriately use and manage IoT devices connected to information systems, including "minimum information security requirements for managing cybersecurity risks associated with such devices" (the "guidelines"). When developing these guidelines, the IoT Bill directs NIST to consider current industry standards, guidelines, and best practices¹¹⁰.

Though the IoT Bill would apply only to the practices of the federal government and federally procured IoT devices, NIST's guidelines are anticipated to eventually set the standard for the

¹⁰⁶ <https://www.ncsc.gov.uk/news/ncsc-and-allies-publish-advisory-on-the-most-commonly-exploited-vulnerabilities-in-2021>

¹⁰⁷ <https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit#:~:text=The%20NCSC's%20Vulnerability%20Disclosure%20Toolkit%20contains%20the%20essential%20components%20you,process%2C%20including%20validation%20and%20triage.>

¹⁰⁸ <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>

¹⁰⁹ https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

¹¹⁰ <https://www.natlawreview.com/article/iot-bill-heads-to-white-house>

private sector as well. Important standards released by NIST on IoT security have been listed in section 4.8.

4.17. Finland Cyber Security labelling scheme

The Finnish Transport and Communications Agency Traficom launched the Cybersecurity label scheme in 2019 which guarantees the consumers that the labelled devices have basic information security features based on ETSI EN 303 645. The Cybersecurity label can be awarded to networking smart devices if the devices meet the certification criteria, based on the specific needs posed by security threats to consumer devices¹¹¹. Finland and Singapore have signed an MoU for recognising the each other's Consumer IoT products that have met the requirements of Cybersecurity with Label 3 and above. Statement of compliance for the Cybersecurity label¹¹² for the IoT products is based on ETSI EN 303 645.

4.18. World Economic Forum (WEF) initiative on IoT Security

World Economic Forum (WEF) carried out a study on IoT Security through a multistakeholder community formed in it known as council of connected world. The community called on some of the world's biggest manufacturers and vendors to take action for better IoT security¹¹³.

The **Statement of Support**¹¹⁴ released by WEF in February 2022 has been endorsed by more than 100 organizations across stakeholder groups – including leading technology companies, industry organizations, civil society groups, and government cybersecurity agencies. The statement has recognized ETSI EN 303 645 standard for consumer IoT Security.

The statement has endorsed the following five capabilities as a global baseline for consumer IoT device Security:

- a. No universal default passwords
- b. Implementing a vulnerabilities disclosure policy
- c. Keeping software updated
- d. Securely communicating
- e. Ensure that personal data is secure

As per the joint statement, these five device capabilities are **found in over 100 standards, specifications and guidelines**¹¹⁵ across the world and establish a minimum level of security which should form the basis of all consumer IoT cyber security standards, specifications and

¹¹¹<https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label>

¹¹² <https://tietoturvamerkki.fi/sites/default/files/media/file/statement-of-compliance-for-the-cybersecurity-label.pdf>

¹¹³<https://www.weforum.org/impact/iot-security-keeping-consumers-safe/>

¹¹⁴<https://cybertechaccord.org/industry-hackers-and-consumers-for-a-global-baseline-for-consumer-iot-security/>

¹¹⁵<https://iotsecuritymapping.com/>

guidelines. Above five guidelines are already the part of the TEC Technical Report *Code of Practice for Securing consumer IoT* released in 2021 (refer section 3.2).

4.19. European Union (EU) Cyber security strategy

In December 2020, the European Commission presented a comprehensive Cybersecurity Strategy for the Digital Decade which aims to respond to the cyber-related challenges posed by increasing digitalisation, the dependence on modern technologies and various complex threats. The Strategy acknowledges cybersecurity as a multi-level issue, proposing a holistic approach. The text is divided into three areas of action: (1) resilience, technological sovereignty and leadership; (2) building operational capacity to prevent, deter and respond; and (3) advancing a global and open cyberspace¹¹⁶.

On September 15, 2022, the European Commission (EC) has also published a Proposal for a Cyber Resilience Act (CRA Proposal) that sets out new rules in the European Union (EU) for software and hardware products and their remote data processing solutions. **The CRA Proposal introduces mandatory cybersecurity-related requirements and reporting obligations, including about product vulnerabilities, for manufacturers, importers, and distributors of such products**¹¹⁷.

5. Security by Design Guidelines

“Secure by design” is the inclusion of security design principles, technology, and governance at each stage of the IoT journey. When an organization looks at creating, deploying, and leveraging connected technology to drive its business, security is required to be integrated at the design level from the devices to applications and updated from time to time to minimize the risk of vulnerabilities and cyber threats.

Security by design relies on well-known system properties: Integrity, Confidentiality, Authentication, Availability & Resilience. These are required to be combined in systems to offer end-to-end security, to comply with future IoT security standards, to counter the potential attacks and to act as cost-effective and safety-effective security protection mechanisms.

- i. **Confidentiality:** Keeping secrets secret (business value of data, privacy) – encryption is the technology of choice.
- ii. **Integrity:** Ensuring unmodified data transport & unmodified software execution.
- iii. **Availability:** Ensuring that the services remain available.

¹¹⁶ <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy#:~:text=It%20demonstrates%20the%20EU's%20commitment,Security%20Union%20Strategy%202020%2D2025.>

¹¹⁷ https://ec.europa.eu/commission/presscorner/detail/en/IP_22_5374

- iv. **Authentication and Authorization:** Verifying identities for source of data/software access control (trusted operations).
- v. **Resilience:** Devices should be designed to withstand attacks and take recovery actions.

TEC has already released a technical report on *Code of Practice for Securing Consumer IoT* as a part of this document (mentioned in brief in section 3.2.1). Based on the study of a number of standards documents mentioned in sections above, following security by design guidelines have been derived –

1. No universal default passwords

- (i) Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
- (ii) Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
- (iii) Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.
- (iv) Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
- (v) When the device is not a constrained device, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable.

2. Implement a means to manage reports of vulnerabilities:

The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum

- (i) contact information for the reporting of issues
- (ii) information on timelines for
 - a. initial acknowledgement of receipt
 - b. status updates until the resolution of the reported issues
- (iii) There must be a deadline for acting on reported vulnerabilities based on the severity and area in which device is deployed.

3. Keep software updated

- (i) The IoT device should have an OTA (Over the air) update mechanism or a secure update port.
- (ii) Devices should be shipped with latest and patched software available. Both device software and configuration should be documented.
- (iii) Software updates should be encrypted and digitally signed. The device should validate the integrity and authenticity of a software update before applying it. A 'fail safe' mechanism is required that will leave a device in a known safe state in the event an update fails.
- (iv) Software updates should be managed by a well-defined update policy to prevent installation of updates with known issues/ vulnerability. Implement an anti-rollback mechanism, to prevent unauthorised reversion to earlier versions with known vulnerabilities.
- (v) It is important to have a mechanism for securely managing the change of device ownership and also managing devices at their end of life.
- (vi) A central database should track software state of all deployed devices. Any unfixable devices should be flagged and isolated as soon as possible.

4. Securely store sensitive security parameters

- (i) Apply the appropriate level of encryption commensurate with the classification of data being stored.
- (ii) Use industry-standard cypher suite, use the strongest algorithms, and use the latest version of an encryption protocol.
- (iii) Secure storage mechanisms can be used to secure sensitive security parameters. Obfuscation methods used to obscure or encrypt security information, without employing hardware-based protection, can be trivially broken. Appropriate mechanisms include those provided by a Trusted Execution Environment (TEE), encrypted storage associated with the hardware, Secure Elements (SE) or Dedicated Security Components (DSC), and processing capabilities of software wherever possible.

5. Communicate securely

- (i) When configuring a secure connection, if an encryption protocol offers a negotiable selection of algorithms, remove weaker options so they cannot be selected for use in a downgrade attack.
- (ii) All unrequired ports (physical and network), interfaces should be disabled.

- (iii) Authenticate peer before sending any data or acting on received data.

6. Minimize exposed attack surfaces

- (i) All test access points on production units must be disabled or locked.
- (ii) Use tamper evident packaging to protect devices within the supply chain.
- (iii) For equipment handling sensitive information, tamper-evident casing should be used along with tamper detection and tamper protection mechanisms.
- (iv) For high-security deployments, consider design measures against side channel attacks such as active masking, obfuscating signals by varying amplitude and/or time domain, Randomised jitter, and delay.
- (v) Mask cryptographic functions and/ or employ dedicated cryptographic modules.
- (vi) Fail gracefully when physical and operational parameters (voltage, temperature, input data size etc) reach their designed limits.
- (vii) All users, software and agents should be provided minimum access rights, just enough to do their job. Applications should be isolated from each other. For example, use sandboxing techniques such as virtual machines, containerisation, Secure Computing Mode (seccomp), etc. Ensure all errors are handled gracefully and any messages produced do not reveal any sensitive information. Ensure 3rd party application software and libraries, whether off-the-shelf or specifically developed, follow these security guidelines wherever possible, including OWASP recommendation on unsecured & outdated components.

7. Ensure software integrity

- (i) Use secure boot functionality, use a multi-stage bootloader (when possible) initiated by a minimal amount of read-only code.
- (ii) Use a hardware-based tamper-resistant capability (e.g., a microcontroller security subsystem, Secure Access Module (SAM) or Trusted Platform Module (TPM)) to store crucial data items and run the trusted applications. During the boot sequence, wherever possible, check that only the expected hardware and peripherals are present and matches the current configuration parameters.
- (iii) Implement a power-on self-test that validates core functions and integrity of firmware prior to execution. Implement a cryptographic chain of trust from the hardware during boot where possible.

8. Boot should fail gracefully

- (i) If it fails should never reveal an elevated permissions interface.
- (ii) Ensure error messages or responses to invalid messages do not expose sensitive data.

9. Ensure that personal data is secure

- (i) Have a proper data classification system in place. Each data item should be protected (strength of encryption and access control) according to its classification.
- (ii) Assess every item of data transmitted by a device based on data classification rating to it. Take into account that collection of data may be more sensitive than individual items and so may be classified differently.

10. Make systems resilient to outages

- (i) Resilience should be built-in to IoT devices and with respective services. In the case of a loss of network, IoT services should remain operating and natively functional having capability to recover in case of restoration of a loss of power. It should be able to return to a network in a formal manner, rather than in a massive scale reconnect. Other measures should also be implemented such as redundancy into services as well as mitigations policy against DDoS attacks.

11. Examine system telemetry data

- (i) Constant monitoring of the device is necessary to handle operational and security issue in time.
- (ii) Ensure all logged data comply with prevailing data protection regulations.
- (iii) All logs and telemetry data should be stored securely before it's sent to monitoring service, while communicating with the telemetry service, service should be authenticated and data should be encrypted.
- (iv) Access to telemetry data should be on need-to-know basis.

12. Make it easy for users to delete user data

- (i) A 'factory reset' function must fully remove all user data/credentials stored on a device.

13. Make installation and maintenance of devices easy

- (i) The user should be privileged with the functionality such that the devices can be restored in default setting and user data can be erased from the device in a simple manner.
- (ii) Implement least privilege to access all systems.

14. Validate input data

- (i) Use secure design and coding techniques. For example, sanitise and validate all input data before processing, prevent buffer overruns, use secure protocols and remove weak encryption ciphers.

15. Device Identity & Strong Credentials

- (i) A device should be uniquely identifiable by means of a factory-set tamper resistant hardware identifier if possible. Each IoT device should have an associated device certificate for authentication. These certificates should be backed by proper certificate management infrastructure to manage issuance, validation, and revocation. (refer section 1.2.1)
- (ii) Use good password management techniques, don't allow weak or repeated password. Passwords should be stored hashed, salted and never in clear text. Store credentials or encryption keys in a Secure Access Module (SAM), Trusted Platform Module (TPM), Hardware Security Module (HSM) / Secure Elements (SE) or trusted key store if possible.
- (iii) Use 2 factor authentication wherever appropriate.
- (iv) Data stored and processed by the device should be classified for sensitivity and secured appropriately.

16. Password policy

- (i) Passwords should be complex, not easily guessable and not to be stored in clear text.
- (ii) Ensure that any system defaults, such as passwords, certificates or keys, are forced to be changed prior to initial operation.
- (iii) Ensure parameters which could compromise the system (secret or private cryptographic keys, passwords, etc.) are unique per device.

- (iv) The device may contain a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

17. Vulnerability testing

The IoT devices should be tested against known vulnerabilities prior to release. To begin with, critical devices and the networking elements may be taken.

6. Classification of IoT devices

To classify devices, an evaluation and certification scheme may be necessary, which should be based on a generic and common framework, possibly with provisions of business or application-specific use-cases. Such a framework should be based on assurance levels and the devices may be classified based upon the risk associated with the applications they host.

A device classification / labelling schemes defined by IoTSF and TEC-TR are detailed in the sections below, and of CSA Singapore in section 4.13.2 of this document. These three labelling schemes have been mapped in section 6.3.

6.1. IoTSF Assurance classes

IoTSF has adopted a risk-based approach derived from the commonly used CIA (Confidentiality – Integrity - Availability) TRIAD mentioned in its document *IoT Security Assurance Framework*¹¹⁸ (Release 3.0, 2021).

This IoT Security Assurance Framework guides its user through a structured process of questioning and evidence gathering. This ensures suitable security mechanisms and practices are implemented. Based on this, IoTSF has defined a framework having five Assurance Classes that achieve progressively higher levels of Confidentiality, Integrity, and Availability as mentioned below:

- Class 0: where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organisation.
- Class 1: where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organisation (requirements in ETSI, DCMS, NCSC CoP Demand Class 1 at a minimum).
- Class 2: in addition to class 1, the device is designed to resist attacks on availability that would have significant impact on an individual or organisation, or impact many individuals. For example, by limiting operations of an infrastructure to which it is connected.

¹¹⁸<https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf>

- Class 3: in addition to class 2, the device is designed to protect sensitive data including Personally Identifiable Information (PII).
- Class 4: in addition to class 3, where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury.

For each assurance class, the levels of integrity, availability and confidentiality are shown in the table below:

Assurance Class	Security Objectives		
	Confidentiality	Integrity	Availability
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

Table 2: Compliance Classes for IoT Device

The definitions of the levels of confidentiality, integrity, and availability are as follows:

- Confidentiality
 - o Basic– devices or services processing public information.
 - o Medium – devices or services processing sensitive information, including Personally Identifiable Information, whose compromise would have limited impact on an individual or organisation.
 - o High – devices or services processing very sensitive information, including sensitive personal data whose compromise would have significant impact on an individual or organisation.
- Integrity
 - o Basic – devices or services whose compromise could have a minor or negligible impact on an individual or organisation.
 - o Medium – devices or services whose compromise could have limited impact on an individual or organisation.
 - o High – devices or services whose compromise could have a significant or catastrophic impact on an individual or organisation.
- Availability
 - o Basic – devices or services whose lack of availability would cause minor disruption.

- o Medium – devices or services whose lack of availability would have limited impact on an individual or organisation.
- o High – devices or services whose lack of availability would have significant impact to an individual or organisation, or impacts many individuals.

6.2. TEC TR device classification

TEC technical report *Recommendations for IoT/ M2M security*¹¹⁹ has mentioned the six levels of classification for end point device classification based on user authentication.

Level 0: No authentication and Identification

Level 1: Identification and Authentication based on defined ID on End Point Device

Level 2: PIN based Authentication and Identification

Level 3: Username and password authentication method

Level 4: Key exchange and mutual authentication method

Level 5: Biometric authentication

The table below recommends certain options for user authentication based on the classification of the Assurance Levels for End Point Devices.

Level	ID	PIN	Username and Password	Authentication PKI Infrastructure	Personalize and Biometric
L0	X	X	X	X	X
L1	✓	X	X	X	X
L2	✓	✓	X	X	X
L3	✓	✓	✓	X	X
L4	✓	✓	✓	✓	X
L5	✓	✓	✓	✓	✓

Table 3 :Classification of devices as per TEC-TR

The following criteria is proposed for assessing the security classification of Use Cases:

- Mission Criticality
 - o Is the assured delivery of data/ information a mandatory requirement?
 - o Is redundancy in data path mandatory?
- Time Criticality
 - o Is the data/ information time critical?
 - o Is Quality of Service aspect mandatory?
- Sensitivity of Data
 - o Does the data exchange impact national security?

¹¹⁹<https://tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20IoT%20M2M%20Security.pdf>

- Is the data being exchanged mission critical?
- Is Personally Identifiable Information being exchanged?

Based on the above, the following classification for the Use Cases is proposed:

- a. Mission Critical, High QoS, Sensitive Information [CQS]
- b. Mission Critical, High QoS, Non-Sensitive Information [CQN]
- c. Non-Critical, Best Effort, Sensitive Information [NBS]
- d. Non-Critical, Best Effort, Non-Sensitive Information [NBN]
- e. Non-Critical, High QoS, Non-Sensitive Information [NQN]

The table below recommends the mandatory security compliance by Use Case Classification:

Use case class	Availability / QoS	Authentication level	Encryption	KYC	
			Transport Layer	Machine	User
CQS	High	L4	Mandatory	Mandatory	Mandatory
CQN	High	L2		Mandatory	
NBS	Low	L3	Mandatory	Mandatory	Mandatory
NQN	High	L1			
NBN	Low	L0			

Table 4 : Classification of use cases

For more details, refer to TEC technical report on *Recommendations for IoT / M2M Security*¹²⁰.

6.3. Mapping of device classifications / labelling scheme

Harmonisation with global standards is important therefore device classification / labelling schemes available in IoTSF, CSA Singapore, and TEC-TR have been mapped. For this, levels available in TEC-TR are being updated as given below without making any impacts on the assurance levels:

Level 0: → Level-ZS –No authentication or Identity verification.

Level 1: → Level-0 - Identification and Authentication based on defined ID on End Point Device

Level 2: → Level-1 - PIN based Authentication and Identification

Level 3: → Level-2 - Username and password authentication method

Level 4: → Level -3 - Key exchange and mutual authentication method

¹²⁰<https://tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20IoT%20M2M%20Security.pdf>

Level 5: → Level -4 - Biometric authentication

The table below has revised recommendation and certain options for the user authentication based on the classification of the Assurance Levels for End Point Devices.

Level	ID	PIN	Username Password	Authentication PKI Infrastructure	Personalize and Biometric
L-ZS	X	X	X	X	X
L-0	✓	X	X	X	X
L-1	✓	✓	X	X	X
L-2	✓	✓	✓	X	X
L-3	✓	✓	✓	✓	X
L-4	✓	✓	✓	✓	✓

Table 5 : Revision of table -4 to align with international standards

Efforts have been made to map the device classifications as available in TEC-TR with the device classifications / labelling scheme available in the reports published by IoTSF and CSA Singapore in the table-6 below:

<i>Device classification available from different standard bodies</i>			TEC TR 2019	L-ZS	L-0	L-1	L-2	L-3	L-4
			IoTSEF 2021	X	Class 0	Class 1	Class 2	Class 3	Class 4
			SG CLS 2021	X	X	Level-1	Level-2	Level-3	Level-4
Security Features	Security Requirements								
Confidentiality	Message Encryption		X	X	X	√	√	√	
	Attack Protection		X	X	X	√	√	√	
	Data Encryption		X	√	√	√	√	√	
	Tamper Resistance		X	X	X	√	√	√	
	Security Assessment Certificates		X	X	X	√	√	√	
	Device ID Management (Physical/ Logical)		X	X	√	√	√	√	
Integrity	Data Integrity		X	X	√	√	√	√	
	Platform Integrity		X	X	X	√	√	√	
	Secure Booting and Integrity Test / Self Test		X	X	X	X	√	√	
Availability	Logging		√	√	√	√	√	√	
	External Attack Prevention & Response		X	X	X	√	√	√	
	Secure Monitoring		X	X	X	X	√	√	
	Secure Firmware Update & Patch Update		X	X	√	√	√	√	
	Software Assets Protection & Response		X	X	X	√	√	√	
	Vulnerability Management & Response		X	X	√	√	√	√	
	Security Policy Update & Response		X	X	X	√	√	√	
Authentication/ Authorization	Biometrics		X	X	X	X	X	√	
	User Authentication		X	√	√	√	√	√	
	Data Authentication		X	X	√	√	√	√	
	Password Management		X	X	√	√	√	√	
	Access Control		√	√	√	√	√	√	
	Device ID Verification		X	X	X	√	√	√	
TEC TR 2019			L-ZS	L-0	L-1	L-2	L-3	L-4	
	IoTSEF	SG CLS	X	Class 0	Class 1	Class 2	Class 3	Class 4	
NBN	Basic	Meet Baseline Security Requirement							
CQN, NBS	Medium	Adherence to International Standards							
CQS	High	Adherence to the principles of Security by Design, absence of known vulnerabilities and life cycle requirement + software binary analysis.							
		Resistance against common cyber attack and undergo for penetration testing							

Table 6: Mapping of device classifications from various standardization bodies

Note: Attributes related to Confidentiality, Integrity, Availability and Authentication / Authorization are based on the research paper “Security Considerations Based on Classification of IoT Device Capabilities” published by Electronics and Telecommunications Research Institute(ETRI) Korea available on

https://www.thinkmind.org/index.php?view=article&articleid=service_computation_2017_2_10_10008.

6.4. Proposed classification for IoT devices in India

From the details available in table-6, it is proposed to have following IoT device classification/ levels / labelling scheme for India: -

- The Level L-ZS may be referred as Level-0.
- The Level L-0 may be merged in L-1 and they be jointly referred as Level-1.
- Levels L-2, L-3 and L-4 will become Level-2, Level-3 and Level-4 respectively.

Proposal for Device Classification						
Security Features	Security Requirements	Level-0	Level-1	Level-2	Level-3	Level-4
Confidentiality	Message Encryption	X	√	√	√	√
	Attack Protection	X	X	√	√	√
	Data Encryption	X	√	√	√	√
	Tamper Resistance	X	X	√	√	√
	Security Assessment Certificates	X	X	√	√	√
	Device ID Management (Physical/ Logical)	√	√	√	√	√
Integrity	Data Integrity	X	X	√	√	√
	Platform Integrity	X	X	√	√	√
	Secure Booting and Integrity Test / Self Test	X	X	X	√	√
Availability	Logging	√	√	√	√	√
	External Attack Prevention & Response	X	X	X	√	√
	Secure Monitoring	X	X	X	√	√
	Secure Firmware Update & Patch Update	X	√	√	√	√
	Software Assets Protection & Response	X	X	√	√	√
	Vulnerability Management & Response	X	√	√	√	√
	Security Policy Update & Response	X	X	X	√	√
Authentication/ Authorization	Biometrics	X	X	X	X	√
	User Authentication	X	√	√	√	√
	Data Authentication	X	X	√	√	√
	Password Management	X	√	√	√	√
	Access Control	√	√	√	√	√
	Device ID Verification	X	X	√	√	√
Security Assement and standard		Level-0	Level-1	Level-2	Level-3	Level-4
Meet Baseline Security Requirement						
Adherence to cyber security based on International Standards						
Adherence to the principles of Security by Design, and absence of known common software vulnerabilities						
Resistance against common cyber-attack and undergo for penetration testing						

Table 7: Proposed levels for IoT devices

1. **Level-0:** Such devices are very constrained devices with very low processing power, no data encryption and message encryption. Such type of devices may not enable a secure communication and should be allowed to work through such gateways which can add the required measure of security. Without the security augmentation by a Gateway, such type of devices should not be permitted for use in mission critical infrastructure. It is required that the Gateways used to connect such devices will follow the security assurance at Level 2 / Level 3.
2. **Level-1:** Devices of this level must use a protocol stack specifically designed for IoT devices with constraints, such as Constrained Application Protocol (CoAP). Device examples in this category can include environmental sensors. Devices in this category should meet the baseline requirements of ETSI EN 303 645 i.e. no default password, ensuring the availability of security updates and implementing means to manage vulnerability reporting.
3. **Level-2:** Security requirement of Level-1 and adherence to international standards (secure identity, software asset security etc.).
4. **Level-3:** Absence of Known Common Software Vulnerabilities. The devices must meet the Security assurance requirements of Level-2 and also the software used in the connected device must be evaluated by a test laboratory using automated binary analysers to ensure that there is no known critical software weakness, vulnerabilities or malware.
5. **Level-4:** The device should perform well against the penetration tests by approved third-party test labs, and fulfil Level-3 requirements. The IoT device undergoes penetration testing by a test laboratory to provide a basic level of resistance against common cybersecurity attacks.

IoT Devices, Products and the networking elements may be classified as per the security assurance requirements stated above, to make it easier for consumers to take informed decisions while procuring and using the devices.

7. Testing and certification programme

The testing and certification of the telecom equipment and IoT devices are being done across the globe by various certification bodies. In India TEC is carrying out testing and certification under MTCTE regime as detailed in section 3.2.5. TEC has already designated a large number of labs across the country. Software and applications testing is being done by STQC as mentioned in section 3.5.1. However, similar program being carried out across the globe is listed below:

7.1. ioXt

The ioXt Alliance has defined its mission to build confidence in Internet of Things products through multi-stakeholder, international, harmonized, and standardized security and privacy requirements, product compliance programs, and public transparency of those requirements and programs. IoT product manufacturers and developers can gain formal

certification to the ioXt global standard through the ioXt Certification Program. The program measures a product for each of the eight ioXt principles with clear guidelines for quantifying the appropriate level of security needed for a specific product. Once approved, the ioXt SmartCert informs end-users, retailers, and ecosystem partners that a product is secure. In ioXt self-certification, IoT manufacturers and developers enter product information directly into the ioXt certification portal to measure against the ioXt standards, while independent researchers validate the submission¹²¹. The eight principles for consumer product design and manufacturing to ensure security, upgradability & transparency are given below :

- No universal passwords
- Secured interfaces
- Proven cryptography
- Security by default
- Signed software updates
- Automatically applied updates
- Vulnerability reporting program
- Security expiration date

7.2. Platform Security Architecture (PSA)

PSA certification provides independent evaluation lab-based assurance of the PSA Root of Trust (PSA-RoT). It features nine predefined security functions, including trusted boot, crypto, secure storage and attestation, to protect the system from common IoT threats. In its role as a trust anchor, the PSA-RoT provides a source of confidentiality and integrity to the whole value chain. Depending on the result of the OEM's threat model, the device maker can choose an appropriate Level (between L1/2/3)¹²². PSA Certified Level 1 aligns with baseline requirements of ETSI EN 303 645 and NIST 8259A ¹²³.

PSA Certified Level 2 provides a laboratory evaluation of a PSA Root of Trust (PSA-RoT) to provide evidence against scalable software attacks¹²⁴.

PSA Certified Level 3 is designed for silicon vendors who want independent evaluation of their PSA Root of Trust (PSA-RoT) implementation, which may give confidence to OEMs and ODMs (Original Design Manufacturers) that the chip can provide protection from hardware and software attacks¹²⁵.

¹²¹<https://www.ioxtalliance.org/get-ioxt-certified>

¹²²<https://developer.arm.com/architectures/architecture-security-features/platform-security>

¹²³[https://www.psacertified.org/getting-certified/device-manufacturer/level-](https://www.psacertified.org/getting-certified/device-manufacturer/level-1/#:~:text=PSA%20Certified%20Level%201%20aligns,Californian%20State%20Law%20SB%2D327.)

[1/#:~:text=PSA%20Certified%20Level%201%20aligns,Californian%20State%20Law%20SB%2D327.](https://www.psacertified.org/getting-certified/device-manufacturer/level-1/#:~:text=PSA%20Certified%20Level%201%20aligns,Californian%20State%20Law%20SB%2D327.)

¹²⁴ <https://www.psacertified.org/getting-certified/silicon-vendor/overview/level-2/>

¹²⁵ <https://www.psacertified.org/getting-certified/silicon-vendor/overview/level-3/>

7.3. Global Certification Forum (GCF)

GCF launched a consumer IoT security accreditation programme, available to manufacturers of consumer IoT product, regardless of membership status within the GCF ecosystem. This programme ensures compliance with requirements mentioned in ETSI EN 303 645 standard for cybersecurity. Consumer IoT products include smart door locks, Smart Cameras, Smart TVs, wearables, connected home automation and appliances, as well as connected toys and baby monitors¹²⁶.

Various test labs have developed testing procedure based on ETSI EN 303 645, NISTIR 8259 and other security related standards such as UL IoT¹²⁷, TUV SUD¹²⁸, SESIP¹²⁹ etc.

7.4. Common Criteria (CC)

Common Criteria is the view that vulnerabilities can arise at any stage of requirement, development and operation in any organisation. It is also having a Common Criteria Recognition Arrangement (CCRA) with members for testing of products in the labs against common criteria specifications. These certificates are recognized by all the signatories of the CCRA.

Common Criteria Protection profile - Protection Profile PP0084 has been developed for “Security IC Platform Protection Profile with Augmentation Packages” [PP0084] defining the Security Targets in order to perform a certification of Security Integrated Circuits.

Secure-Sub-System in System-On-Chip (3S in SoC) Protection Profile PP0117 has been released in 2022.

Common Criteria has designed some of the evaluation schemes as detailed below:

EAL1 – Functionally Tested – It provides a basic level of assurance by a limited security target and an analysis of the Security Function Requirements (SFR) in that Security Targets using a functional and interface specification.

EAL2- Structurally Tested – A basic description of the architecture of the Target of Evaluation (TOE), to analyse the security behaviour.

EAL3 - Methodically tested and checked – This level provides assurance by a full security target and an analysis of the Security Function Requirements (SFR) in that Security Targets (ST), using a functional and interface specification.

¹²⁶<https://www.globalcertificationforum.org/news/consumer-iot-security-programme-launched.html>

¹²⁷ <https://www.ul.com/news/uls-iot-security-rating-helps-demonstrate-product-security-marketplace>

¹²⁸ <https://www.tuvsud.com/en-gb/services/cyber-security/iot-device-cybersecurity>

¹²⁸ https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/04-03-pandza#:~:text=T%C3%9CV%20Rheinland%20offers%20certification%20against,fully%20includes%20EN%20303%20645.

¹²⁹ <https://globalplatform.org/sesip/>

EAL4 – Methodically designed, tested, and reviewed – It permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises, also provides assurance through the use of development environment controls and additional Target of Evaluation (TOE) configuration management including automation, and evidence of secure delivery procedures.

EAL5– Semiformally designed and tested– It provides increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analysable) architecture.

EAL6 – Semiformally verified design and tested – It provides increase in assurance from EAL5 by requiring more comprehensive analysis, a structured representation of the implementation, more architectural structure (e.g. layering), more comprehensive independent vulnerability analysis, and improved configuration management and development environment controls.

EAL7 –Formally verified design and tested– It provide increase in assurance from EAL6 by requiring more comprehensive analysis using formal representations and formal correspondence, and comprehensive testing.

7.5. TrustCB

TrustCB¹³⁰ is a commercial Certification Body that is said to provide high-assurance certification in a predictable, short timeframe. TrustCB specialises in certifying IT security products (and associated sites, processes and services) evaluated according to international and industry standards. TrustCB experience in the certification and evaluation fields enables to extrapolate the rigour of the Common Criteria certification process (Refer section 7.4), and templatise and tailor it to other verticals such as passive RFID and the automotive sector.

7.6. GSMA eUICC Security Assurance (GSMA eSA) Scheme

GSMA in collaboration with industry stakeholders and TrustCB has developed eUICC Security Assurance Scheme¹³¹ which was released in 2021. This scheme aims to provide assurance and trust to the telecom service providers on the embedded SIM (eSIM/eUICC) products produced by the eSIM vendors. eUICC Security Assurance (eSA) is based on the Common Criteria approach to security assurance where the security objectives within the GSMA Protection Profiles (i.e. SGP.05 (for M2M devices) and SGP.25 (for Consumer devices)) still apply. It defines a more dynamic set of procedures for the security evaluation of eUICCs .

¹³⁰<https://trustcb.com>

¹³¹https://www.gsma.com/esim/wp-content/uploads/2021/02/eSA-Scheme-Step-by-Step-Guide_.pdf

8. Summary and Recommendations

Existing policies, standards and guidelines related to M2M/ IoT Security in India and globally have been studied and brief is available in section 3 and section 4 respectively. Key principles for security by design have been covered in section 5. Classification of devices/ labelling scheme has been elaborated in section 6, and testing & certification in section 7. Based on this, following are recommended:

8.1. 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 onboarding 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. 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 (QKD) 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.).

8.3. 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).

8.4. 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. Abbreviations

S.No.	Abbreviation	Full Form
1.	3GPP	3 rd Generation Partnership Project
2.	APT	Asia-Pacific Telecommunity
3.	AWG	APT Wireless Group
4.	BIS	Bureau of Indian Standards
5.	CCTV	Closed Circuit Television
6.	CEN	European Committee for Standardization
7.	CENELEC	European Committee for Electrotechnical Standardization
8.	DDoS	Distributed Denial-of-Service
9.	DoT	Department of Telecommunications
10.	DSRC	Dedicated Short Range Communication
11.	ER	Essential Requirements
12.	eSIM	Embedded Subscriber Identification Module
13.	ENISA	European Union Agency for Cybersecurity
14.	ETSI	European Telecommunication Standards Institute
15.	FTTH	Fiber To the Home
16.	GCF	Global Certification Forum
17.	GPON	Gigabit Passive Optical Network
18.	GR	Generic Requirements
19.	GSMA	Global System for Mobile communications Association
20.	ICT	Information and Communication Technology
21.	IEC	International Electrochemical Commission
22.	IEEE	Institute of Electrical and Electronics Engineer
23.	IoT	Internet of Things
24.	IoTSEF	Internet of Things Security Foundation
25.	IoXt	Internet of Secure Things
26.	IPv4/IPv6	Internet Protocol version 4/version 6
27.	IR	Interface Requirements
28.	ISO	International Organization for Standardization
29.	ITU	International Telecommunication Union
30.	ITU-T	ITU's Telecommunication Standardization Sector
31.	LTE	Long Term Evolution
32.	M2M	Machine to Machine
33.	MoHUA	Ministry of Housing and Urban Affairs
34.	M2M-SP	M2M Service Provider
35.	MTCTE	Mandatory Testing & Certification of Telecom Equipment
36.	NDCP	National Digital Communications Policy
37.	NIST	National Institute of Standards and Technology
38.	NTC	National Trust Centre
39.	PLC	Power Line Communication
40.	PSA	Platform Security Architecture
41.	TEC	Telecommunication Engineering Centre
42.	TRAI	Telecom Regulatory Authority of India
43.	TSDSI	Telecommunications Standards Development Society of India
44.	WEF	World Economic Forum
45.	Wi-Fi	Wireless Fidelity

10. Annexures

10.1. Annexure-I: Important standards

Standard Number	Title
ITU-T Y.2720	NGN identity management framework
ITU-T Y.3056	Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems
ITU-T Y.3051	The basic principles of trusted environment in ICT infrastructure.
ITU-T Y.3052	Overview of trust provisioning for information and communication technology infrastructures and services
ITU-T Y.4500.1	Recommendation ITU-T Y.4500.1 (2018), oneM2M – Functional architecture.
ITU-T Y.4500.3	oneM2M – Security solutions
ITU-T Y.4800	Requirements and functional architecture of an automatic location identification System for ubiquitous sensor network applications and services
ITU-T Y.4802	Multimedia information access triggered by tag-based identification–Registration procedures for identifiers
ITU-T Y.4804	Multimedia information access triggered by tag-based identification– Identification scheme
ITU-T Y.4806	Security capabilities supporting safety of the Internet of things
ITU-T Y.4807	Agility by design for telecommunication/ ICT systems security used in the IoT
ITU-T Y.4810	Requirements for data security of heterogeneous Internet of things devices
ITU-T X.509 (10/2019)and cor.1 (10/2021)	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
ITU-T X.510	Information technology - Open Systems Interconnection - The Directory: Protocol specifications for secure operations
ITU-T X.667	Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers
ITU-T X.1252	Baseline identity management terms and definitions
ITU-T X.1254	Entity authentication assurance framework
ITU-T X.1361	Security framework for the Internet of things based on the gateway model
IS 17737 (Part 1):2021	Mobile Device Security
IS/ISO/IEC 27007: 2017	Information security cybersecurity and privacy protection Guidelines for information security management systems auditing.

Standard Number	Title
IS/ISO/IEC 27033-4: 2014 (Reaffirmed In : 2019)	Information technology –Security techniques –Network: Security: Part 4 Securing communications between networks using Security gateways.
ISO 16100-1	Industrial automation systems and integration – Manufacturing software capability profiling for interoperability – Part 1: Framework
ISO/IEC 27000:2018	Information technology, Security techniques, Information security management systems- overview and vocabulary.
ISO/IEC TS 27008:2019	Guidelines for assessment of information security controls.
ISO/IEC 27001	Requirements for an information security management system (ISMS).
ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection – Information security controls.
ISO 27036	Information security for supplier relationships.
ISO 27400 : 2022	Cybersecurity – IoT security and privacy – Guidelines
ISO 28000	Security management systems for the supply chain.
ISO/IEC 29100	Information technology – Security techniques – Privacy framework
ISO/IEC 30141:2018	Internet of Things (IoT) – Reference Architecture
IEC 62443	Series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS)
ETSI TS 103 645	Cyber Security for Consumer Internet of Things: Baseline Requirements
ETSI EN 303 645	Cyber Security for Consumer Internet of Things: Baseline Requirements
ETSI TS 103 701	Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
ETSI TR 103 621	Guide to Cyber Security for Consumer Internet of Things
ETSI TS 103 848	Cyber Security for Home Gateways
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations
NISTIR 8228	Consideration for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
NIST SP 800-213	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements
NISTIR 8259	Foundational Cybersecurity Activities for IoT Devices Manufacturers
NISTIR 8259A	IoT Device Cybersecurity Capability Core Baseline
NISTIR 8425	Profile of the IoT Core Baseline for Consumer IoT Products
GSMA CLP.12	IoT Security Guidelines for IoT Service Ecosystems
GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC

Standard Number	Title
GSMA SGP.22	Remote SIM Provisioning (RSP) Architecture for consumer Devices
GSMA SGP.31	eSIM IoT Architecture and Requirements
IETF RFC 5280	IETF RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

- TEC standards related to telecommunication equipments are available on TEC website <https://tec.gov.in/standards-specifications>.
- TEC ERs (Essential Requirements) and ITSAR (Indian Telecommunication Security Assurance Requirements) of telecom products are available on MTCTE portal <https://www.mtcte.tec.gov.in/>.
- The important standards and the ERs related to the telecom products and IoT devices being used in smart cities have been listed in annexure -5 of TEC Technical Report on *IoT/ICT Standards for Smart Cities (TEC 31178:2022)* available at <https://tec.gov.in/M2M-IoT-technical-reports>.
- The DoT has released the Standard Operating Procedure (SoP) for Personalisation of SIM cards vide letter no. 800-04/2017/AS.II dated 16.07.2021 available at <https://dot.gov.in/sites/default/files/SOP%20for%20Personalisation%20of%20SIM%20cards.pdf?download=1>

10.2. Annexure-II: Some examples of threats and their treatment

Threat	Threat Example	Treatment examples
Spoofing	Address resolution protocol (ARP) spoofing used to redirect data traffic to the attacker	Update the software / firmware of the devices to prevent vulnerability exploitation
Tempering	Tampering with software to modify permissions, install spyware or backdoors	Secure boot and update to ensure software and hardware are only modified by trusted sources. Periodic auditing of firmware to check for tampering or unauthorized modification
Repudiation	Sensor data is modified in transit to the cloud service and Enterprise metrics are affected	Use of digital certificates to support secure identity of users and devices Public key infrastructure to manage and revoke digital certificates and roots of trust
Information Disclosure (Data Breach)	Diagnostics information shared with an OEM which discloses proprietary Enterprise information which is not required by the OEM	Traffic monitoring and management (ingoing and outgoing) Separating business and IoT networks
Denial of service	Using exploits in connected devices to execute a DoS or DDoS attack on another IoT device in the Enterprise network	Traffic monitoring, auditing and management (on the IoT network, ingoing and outgoing) Use of gateways and firewalls to monitor and block traffic
Elevation of Privilege	Unauthorized access of a cloud service provider's system enabling access to the Enterprise business or IoT network	Separation of IoT and business networks to discourage privileged users from accessing non-relevant business information

10.3. Annexure-III: Consumer IoT Vulnerabilities and the relevant capabilities as an example

Vulnerability	Relevant Consumer Profile Capabilities
1. Mirai Malware Variants Attacks – Use of weak authentication to enable the loading of malware onto the device and use that device in DDOS and other attacks.	
Unauthorized access to the IoT device Asset Identification	Asset Identification Interface Access Control Information Dissemination Education and Awareness
Malicious code can be loaded on the IoT device	Software Update Cybersecurity State Awareness Education and Awareness
Commands can be launched using the device Interface Access Control	Interface Access Control Documentation
2. Unauthorized Publication of Fitness Tracker Data – Fitness tracker location data for military personnel were publicly posted even when product was configured for privacy.	
Web application vulnerabilities Product configuration	Product configuration Cybersecurity State Awareness Documentation Information Dissemination
Mobile application vulnerabilities	Product Configuration Cybersecurity State Awareness Documentation Information Dissemination
Ability for de-identified data to be re-identified	Product Configuration Data Protection Documentation
3. Unauthorized access to home security camera data – Unauthorized access to data and views of the inside and outside of buildings occurred with multiple brands of security cameras.	
Weak authentication	Interface Access Control
Unauthorized data sharing	Data Protection Documentation Information Dissemination
Non-responsive to questions and complaints to the developers	Information and Query Reception
Lack of monitoring capabilities and procedures	Asset Identification Product Configuration Documentation
Lack of data recording/collection controls	Asset Identification Product Configuration Documentation Information Dissemination Education and Awareness

[Source: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf>]

Table 8: Consumer IoT Vulnerabilities and the Relevant Capabilities

10.4. Annexure-IV: Use of ITU-T X.509 standard in digital certificates

X.509 based certificates are being used for various types of digital transactions, some such scenarios are as listed below:

- i. **TLS/SSL Certificates:** The X.509 standard is used in TLS/SSL certificates, which underpin the https protocol used in websites.
- ii. **S/MIME Certificates:** X.509 standard makes email secure by powering S/MIME certificates. These certificates verify email senders to help protect against phishing attacks and encrypt email messages to provide a layer of security for messages so that we know what we received wasn't modified in transit. As a result, X.509 certificates have played a huge role in making email such a trustworthy mode of communication.
- iii. **Digital Signatures:** X.509 standard gets used to verify the identity of the signer and to ensure that the document doesn't get altered in transit before or after signature.
- iv. **Code Signing:** X.509 certificates support code signing similarly to how they support digital signatures since a code signing certificate verifies the identity of the developer and the company and protects against modification to the program that gets delivered.

Use of X.509 certificate in PKI based identification and authentication is being used by several IoT platform for proving secure services as listed below:

Device Manufacturing and Provisioning with X.509 Certificates in AWS IoT Core¹³²

AWS IoT Core supports TLS-based mutual authentication using X.509 certificates to protect and encrypt data in transit from an IoT device to AWS IoT Core. Device makers must provision a unique identity, including a unique private key and X.509 certificate, into each device. Device makers must also set up the necessary cloud resources on Amazon Web Services (AWS) for each device.

Device Provisioning Services with X.509 certificates in Microsoft Azure

Microsoft Azure is using X.509 certificates for its Device Provisioning Services(DPS) on its cloud platform¹³³.

¹³² <https://d1.awsstatic.com/whitepapers/device-manufacturing-provisioning.pdf>

¹³³ <https://learn.microsoft.com/en-us/azure/iot-dps/quick-enroll-device-x509?pivots=programming-language-csharp>

10.5. Annexure-V: Important links related to e-SIM [Source: GSMA]

1. SM-DP/SM-SR

List of SM-DP and SM-SR that have been accredited with the SAS are available on the link: <https://www.gsma.com/security/sas-accredited-sites/>

2. List of FAB/E-SIM manufacturer

List of EUMs(eUICC Manufacture) that have been accredited with SAS are available on the link: <https://www.gsma.com/security/sas-accredited-sites/>

List of EUM product that have been certified according to Global Platform are available on the link <https://globalplatform.org/certified-products/?filter-certification-type=functional>

3. Certifying agency

The certifying agencies for SAS are available on the link <https://www.gsma.com/security/sas-auditors/>

The certifying laboratories for the Functional certification are available on the link https://globalplatform.org/laboratories/?utm_source=iseepr&utm_medium=Website&utm_campaign=Secure%20Component

List of virtual meetings of the Working Group

S.No.	Date of virtual meeting
1.	04 th July 2019
2.	12 th July 2019
3.	11 th September 2019
4.	18 th November 2019
5.	18 th December 2019
6.	06 th January 2020
7.	20 th January 2020
8.	18 th February 2020
9.	19 th March 2020
10.	16 th April 2020
11.	15 th May 2020
12.	16 th June 2020
13.	27 th July 2020
14.	03 rd September 2020
15.	25 th September 2020
16.	12 th October 2020
17.	12 th November
18.	11 th December 2020
19.	22 nd December 2020
20.	13 th January 2021
21.	19 th February 2021
22.	13 th April 2021
23.	23 rd April 2021
24.	07 th May 2021
25.	29 th June 2021
26.	29 th July 2021
27.	10 th August 2021
28.	31 st August 2021 - Release of <i>Code of Practice for Securing Consumer IoT</i>
29.	01 st October 2021
30.	05 th October 2021
31.	06 th January 2022
32.	08 th February 2022
33.	11 th March 2022
34.	24 th March 2022 - Release of <i>Framework for National Trust Centre</i>
35.	17 th May 2022
36.	28 th June 2022
37.	08 th August 2022
38.	09 th September 2022
39.	22 nd September 2022
40.	14 th October 2022
41.	21 st November 2022
42.	23 rd December 2022
43.	10 th January 2023
44.	24 th January 2023
45.	23 rd February 2023



ISO 9001 :2015

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