

*IoT Security
Roadmap*

Table of Contents

- 1. VISION AND OBJECTIVES..... 3
 - 1.1. Vision.....3
 - 1.2. Objective 3

- 2. CONTRIBUTORS 6

- 3. PATRONS 6

- 4. INTRODUCTION 9
 - 4.1. OverviewError! Bookmark not defined.
 - 4.2. Importance of Security in IoT environment.....Error! Bookmark not defined.

- 5. IOT SECURITY.....13
 - 5.1. Hardware Level Security 16
 - 5.2. Network Level Security 20
 - 5.3. Application-Level Security..... 22
 - 5.4. Security in IoT Operating System..... 23

- 6. NATIONAL AND INTERNATIONAL IOT SECURITY STANDARDS.....24

- 7. IOT APPLICATION DOMAINS AND SECURITY ISSUES34
 - 7.1. Smart Home 34
 - 7.2. Smart City 34
 - 7.3. Smart Agriculture..... 35
 - 7.4. Smart Grid 35
 - 7.5. Healthcare 36
 - 7.6. Industrial IoT..... 39
 - 7.7. Security in Automotive 45

- 8. IOT SECURITY: FUTURE AND TRENDS49

- 9. PROPOSED ROADMAP54
 - 9.1. Ongoing Activities 54
 - 9.2. Short Term (Next 5 years)..... 56
 - 9.2.1. IoT Security Sandbox.....56
 - 9.2.2. eSIM Cellular-IoT59
 - 9.2.3. IoT Device Certificate Lifecycle Management62
 - 9.2.4. IoT Identification63
 - 9.2.5. IoT Protocols66
 - 9.2.6. IoT Access Controls68
 - 9.2.7. Lightweight Cryptography69

9.2.8.	IoT Network Security Orchestration and Automation.....	71
9.2.9.	oneM2M	73
9.2.10.	MLOps and Decentralized AI/ML pipelines	74
9.2.11.	Blockchain assisted IoT Security.....	78
9.2.12.	Theft and Tampering of IoT devices	79
9.2.13.	New Chip design and Standards.....	81
9.2.14.	Artificial Intelligence of Things (AIoT)	81
9.2.15.	Zero-Trust Architecture	82
9.2.16.	AI Enabled Privacy and Data Protection	83
9.2.17.	Self-Adapting Intrusion Detection System	85
9.2.18.	IoT and IoTA Tangle Distributed Ledger.....	86
9.2.19.	High Performance Computing (AI capable) devices for the edge	87
9.2.20.	5G and IoT	88
9.2.21.	Enhancement in the Automotive Security	90
9.3.	Mid Term (Next 10 years).....	92
9.3.1.	Trusted Components and Reusable Certifications	92
9.3.2.	PQC Enabled IoT System	92
9.3.3.	Low-power Quantum Random Number Generator (QRNG)	93
9.3.4.	AI Enabled Botnet Detection and DNS Ecosystem	94
9.3.5.	5G and 6G Transition Security	96
9.3.6.	Self-sufficient Intelligent Network (AI)	97
9.3.7.	Satellite Connectivity	97
9.3.8.	RISC-V based Secure SoC for IoT	97
9.3.9.	UAV assisted Wireless Communication.....	98
9.3.10.	Digital Twin.....	98
9.3.11.	Collective Intelligence: AI-Enhanced Automotive Security and Threat Anticipation	99
9.3.12.	Automotive Supply Chain attacks – Risk mitigation strategies.....	100
9.4.	Long Term (up to 2040)	101
9.4.1.	Secure IoT Network through QKD and SDN	101
9.4.2.	Federated Machine Learning and Swarm Learning.....	102
9.4.3.	Self-aware IoT Protocols and its Security	103
9.4.4.	Low power PQC.....	105
9.4.5.	Low power to No power cryptography algorithm for IoT	105
9.4.6.	Deterministic Response for IIoT and Automotives.....	107
9.4.7.	Zero Knowledge Proof.....	109
10.	TIMELINES: FROM RESEARCH TO MATURE SOLUTIONS	110
11.	CONCLUSION.....	113
12.	REFERENCES.....	114

1. Vision and Objectives

1.1. Vision

As digital technologies increasingly embrace all parts of society and industry, the digital and physical worlds are entangled in new, complex ways. The Internet of Things (IoT) and the recent developments are narrowing the gap between the virtual and physical worlds. The advantages of IoT technology could be realized by facilitating the secure adoption of IoT solutions. The vision of IoT security roadmap is to establish a resilient and dependable environment in which interconnected devices and systems are safeguarded against various forms of attacks/threats, hence guaranteeing the confidentiality, Integrity, authenticity, and accessibility of data and services. The incorporation of security measures is a critical component of the design and execution of IoT systems, as opposed to being seen as a secondary consideration. The process encompasses the advancement of devices and networks that prioritize security from the outset, along with the incorporation of extensive security standards and optimal methodologies. It may require a renewed look into IoT design where functionality has to be fused with security i.e., secure by design.

1.2. Objective

While there is a plethora of past and ongoing research on IoT security, the constant and rapid evolution of IoT technologies and cyber-attacks requires consistent investment in these areas. In this respect, research should focus on ‘intelligent’ approaches to security, i.e., on the ability to ‘learn’ new attack patterns and derive counter solutions autonomously. Beyond cyber security for IoT, trust in IoT solutions and data generated by devices is becoming an important trend in the market. Solutions are focused on providing ways to produce and consume IoT data by highly decentralized and loosely coupled parties through secure traceability mechanisms such as blockchain. IoT devices experience an average of 5200 attacks per month with routers and connected cameras accounting for 90% of the activity. Therefore, maintaining the CIA triad- confidentiality, integrity, and availability is quite essential for deploying IoT applications.

When considering solutions for IoT security, it is imperative to address three fundamental challenges. One of the primary factors contributing to this phenomenon is the widespread use of various connectivity standards, device firmware/operating systems, and use cases. The security field necessitates the ability to function effectively among various potential combinations and variations. Consequently, users of the IoT necessitate a standardized and systems-oriented methodology that is the foundation for effective integration and customization.

Furthermore, it is vital for designers to operate under the assumption that IoT devices and apps will function autonomously without human supervision. It may be necessary to adopt a distinct cognitive framework when engaging with human users in interactive systems, such as those found in telephony and various enterprise IT systems. In the context of the IoT, it is critical to incorporate security measures during the initial design phase and automate various security processes that are often reliant on human interaction. Therefore, there is a need to build a coherent architecture for IoT systems.

The task of developing efficient security solutions for IoT systems may be approached within the framework of a comprehensive architecture that encompasses a wide range of potential scenarios. By comprehensively examining many IoT applications in diverse sectors, scholars and industry professionals have discerned the constituent components of a distributed architecture and a standardized set of service functions essential for implementing IoT systems.

In general, IoT devices tend to have extended operational lifespans. Furthermore, it is worth noting that there could be constraints on the availability of access or the feasibility of physical replacement. On the contrary, user expectations exhibit a rapid pace of evolution that mirrors the dynamism observed in the consumer market. Consequently, it is imperative for security measures to address and reconcile these temporal disparities. The implementation of life-cycle management and cost-efficient security management technologies is contingent upon the adoption of standardization, as it is more probable to yield such outcomes.

The objective of this roadmap is to aid government bodies and other stakeholders in their efforts to:

- Prepare for and take charge of the advancement of next-generation IoT technology. It includes understanding its connection to computing, trust, security, and privacy within the framework of new technologies.
- Establishing an emergency response environment that facilitates efficient security monitoring and the dissemination of advisories.
- Guide the need for India's digital technologies related to a Trusted and Secure IoT ecosystem. (data, cybersecurity, AI, skills, interoperability, etc.) in industry and the public sector.
- Develop a framework and policies to enforce tight privacy requirements for data security in the deployment environment.
- To establish a testbed that standardizes and assesses the security of multi-radio, multi-platform, multi-OS, and multi-topology IoT deployments, as well as to certify the IoT stack as a security complaint.
- It is essential to participate in relevant events organized by prestigious organizations such as the Telecommunications Standards Development Society (TSDSI), Bureau of Indian Standards (BIS), and International Telecommunication Union (ITU), etc. to actively engage and make valuable contributions to standardization initiatives at both the national and international levels.
- Support projects that foster trust in IoT adoption through cybersecurity and privacy-by-design, as well as raise ethical and privacy awareness. Go beyond "meta" Operating Systems, focusing on semi-autonomous orchestration. In the long run, move from centralized orchestration towards decentralized coordination with AI developments to increase autonomy.

2. Contributors

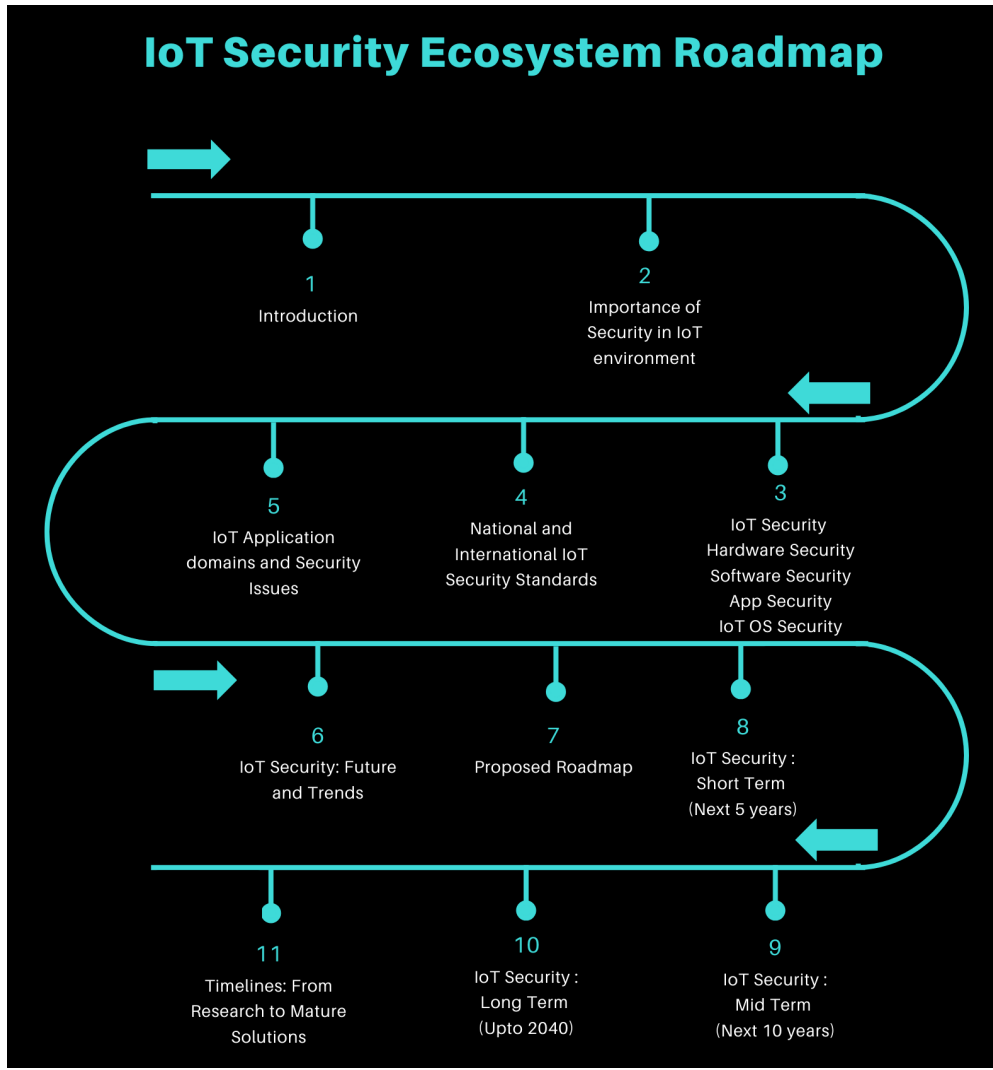
- Mr. Hari Babu Pasupuleti, Mr. Shrikrishna S Chippalkatti, Dr. Vishal J. Rathod, and Mr. M Rohith Reddy, Centre for Development of Advanced Computing (C-DAC), Bangalore
- Centre for Development of Advanced Computing (C-DAC), Chennai
- Centre for Development of Advanced Computing (C-DAC), Hyderabad
- Centre for Development of Advanced Computing (C-DAC), Silchar
- Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram
- Indian Institute of Technology, Madras, Chennai
- Indian Institute of Technology, Bombay
- International Institute of Information Technology, Bangalore
- Society for Electronic Transactions and Security, Chennai
- ERNET, Chennai
- Mr. Tarun Pandey, Scientist-D, Cybersecurity R & D, MeitY, Govt. of India.
- Mr. Pranjal Johri, Scientist-C, Cybersecurity R & D, MeitY, Govt. of India.
- Dr. Prabhakar Krishnan, Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri-campus, Kollam

3. Patrons

- Shri S. Krishnan, Secretary, MeitY, Govt. of India.
- Shri Bhuvnesh Kumar, Additional Secretary, Cyber Security R & D, MeitY, Govt. of India.
- Ms. Tulika Pandey, Scientist-G, Senior Director, Group Coordinator – Cybersecurity R & D, MeitY, Govt. of India.

- Shri Magesh Ethirajan, Director General, Centre for Development of Advanced Computing (C-DAC), India.
- Dr. S. D. Sudarsan, Executive Director, Centre for Development of Advanced Computing (C-DAC), Bangalore, India.

Flow of IoT Security Roadmap Document



IoT security roadmap document is organized in the following manner: Section IV provides brief introduction of IoT and importance of security in IoT network, Section V provides a concise overview of IoT security, encompassing device-level, network-level, and application-level considerations. The ensuing sections VI and VII provide descriptions of security in healthcare, Industrial IoT, and automation. Section VIII provides a comprehensive analysis of the present trends and future prospects pertaining to the security of the Internet of Things (IoT). Section IX outlines the suggested strategic plan in relation to short-term, medium-term, and long-term objectives. The Timeline and Conclusion are provided in Sections X and XI, respectively.

4. Introduction

The Internet of Things (IoT) concept might be interpreted variably among individuals, although it indisputably encompasses many interconnected devices and a substantial volume of data. According to a projection made by the International Data Corporation (IDC), it is anticipated that by the year 2025, there will be a total of 41.6 billion IoT devices in existence. These devices are expected to possess the capability of generating an estimated 79.4 zettabytes (ZB) of data. Therefore, ensuring security is of paramount importance due to the presence of vital data inside this vast dataset [1]. Figure 1 illustrates the global forecast of connected IoT devices.

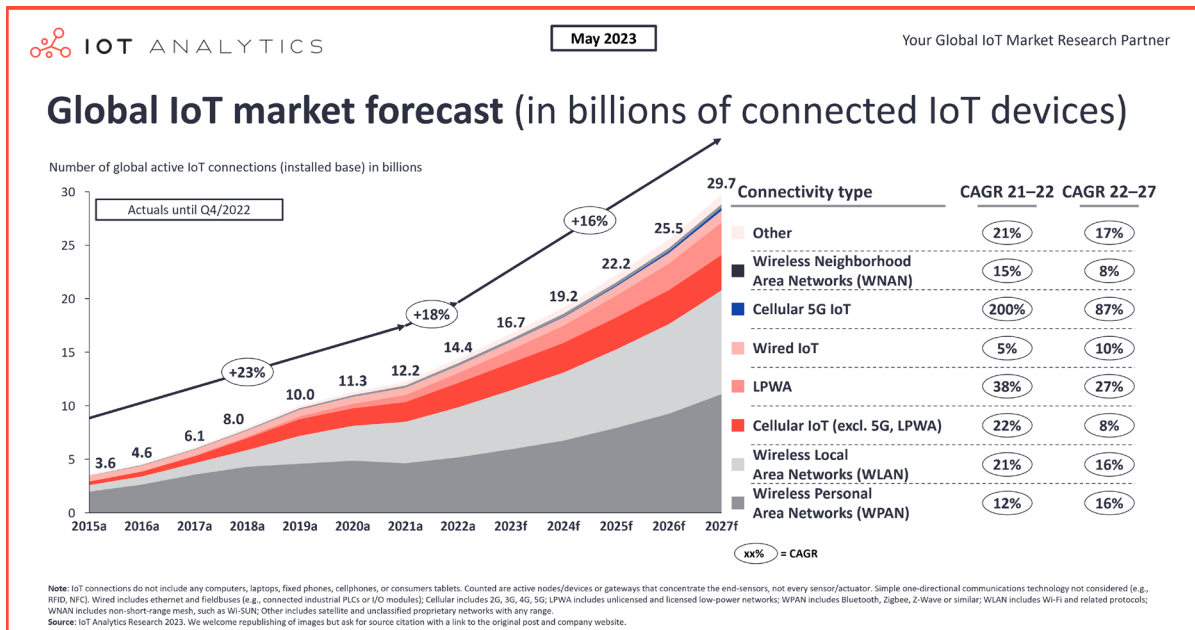


Figure 1: Total number of IoT devices [1]

Several organizations and projects worked on defining reference architectures (as shown in Figure 2) for IoT systems. Defining a new reference architecture is out of scope. Large-scale pilots have consolidated their efforts in an interesting 3D reference model [2] that combines architectural layers, non-functional properties, and cross-cutting functions.

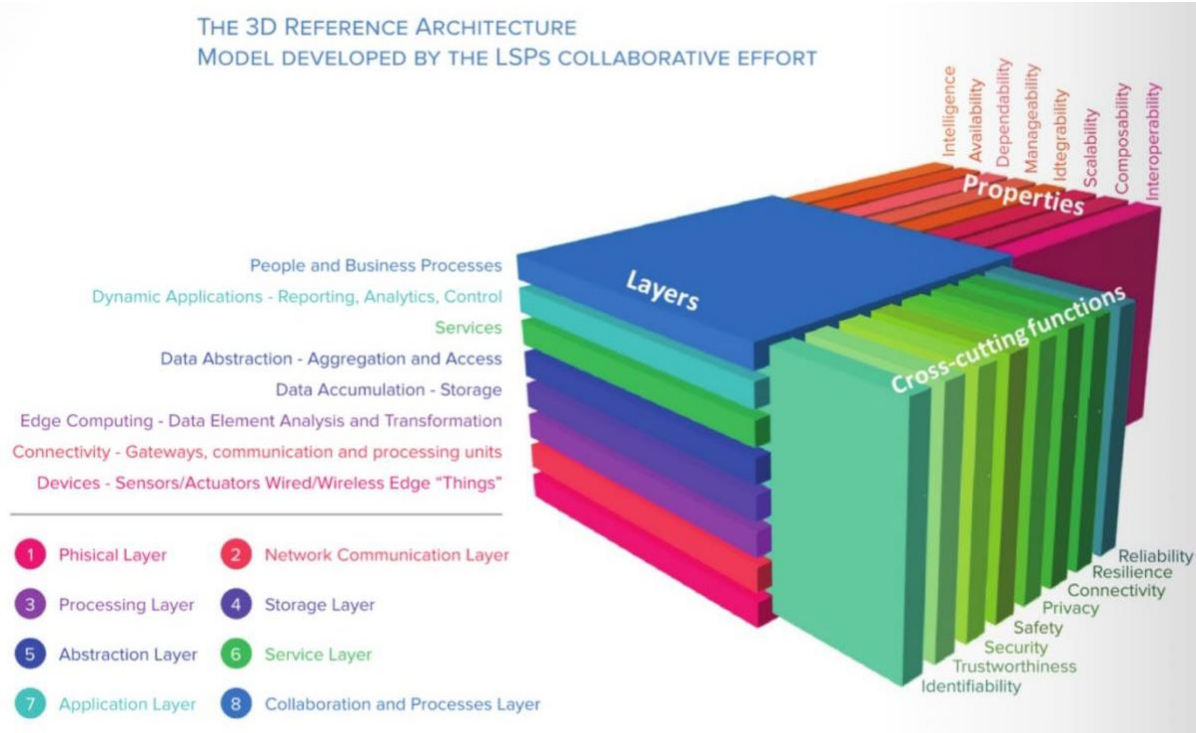


Figure 2: IoT architecture [2]

The Indian landscape is very active in evolving Internet of Things and related technologies seeing it as central, supports a wide set of research policies related to the area. A critical challenge for the upcoming years is the need to ‘leverage technological strength to develop the next generation of IoT devices and systems’ taking full advantage of the key enabling technologies of 5G/6G, trust and cyber-security, distributed computing, cloud architectures, Artificial Intelligence (AI), Machine Learning, and Advanced Computing to build a sustainable and competitive ecosystem in IoT area to ensure ‘end-user trust, adequate security and privacy by design’ covering all the relevant aspects of interoperability, including architectures, devices and tactile/contextual.

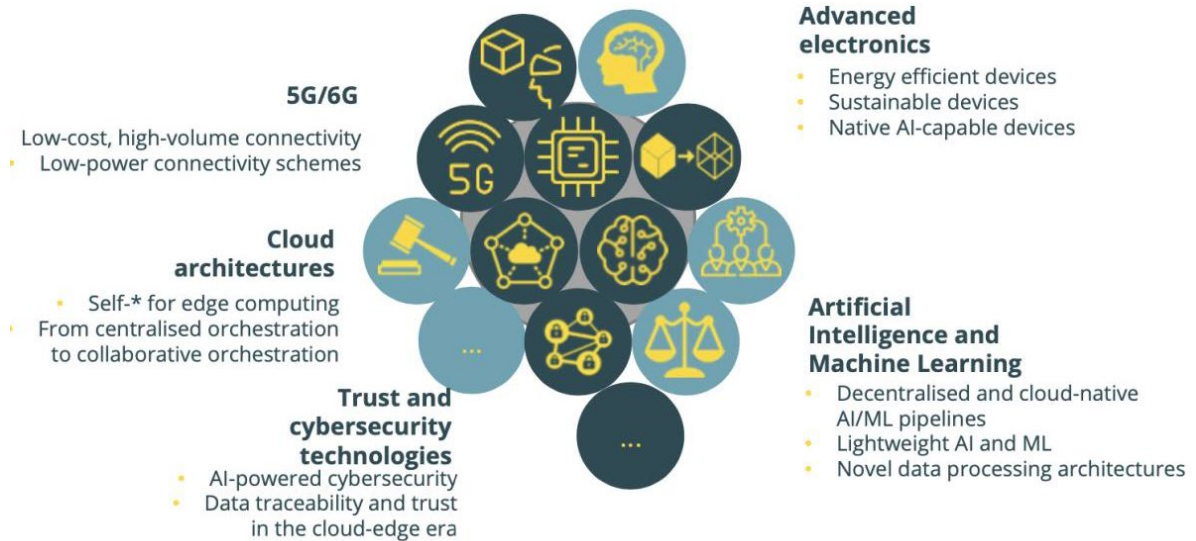


Figure 3: Key technologies enable and research areas.

In this context, key technology enablers for realizing the Next Generation Internet of Things have been identified as:

- 5G/6G:** This technology enabler refers to the new generation of mobile communication that supports a massive number of devices with a diverse range of speed, bandwidth, and quality of service. The fifth generation of mobile cellular technologies encompasses reliability, latency, scalability, security and ubiquitous mobility. The 5G Observatory divides the service in 3 big scenarios according to the application needs (GSMA, 2019), Enhanced Mobile Broadband (EMBB), massive Machine Type Communications (MMTC) and Ultra Reliable Low Latency Communications (URLLC). MMTC promises to allow cheap, reliable and scalable internet connectivity, which is a key requirement for several IoT scenarios. With its augmented spectrum, 5G aims to tackle requirements posed by IoT large deployments beyond what today is possible with Low Power Wide Area Networks (LPWAN), achieving massive and critical communications with a complete vision deployed by 2021 (Nokia Bell Labs, 2019).
- Artificial Intelligence and Machine Learning:** Blended with IoT, AI offers augmented intelligence in the data analysis process. The availability of massive data sets to train, test and apply AI combined with increasing High-Performance Computing (HPC) capability enabled its wide adoption in several real-life scenarios.

The combination is expected to kick off the next wave of performance improvements, especially in the industrial sector by enabling extraction of unexpected ‘intelligence’ from sensed data, the automatic actuation based on ‘intelligent’ models (e.g., self-driving cars), the higher automation in the management of a plethora of devices and their generated data. Also, as Artificial Intelligence becomes a reality across several applications, its combination with IoT is moving towards the edge, enabling the usage of algorithms closer to the devices.

- **Cloud technologies:** while the increasing transition toward edge will reduce adoption of traditional cloud providers, the role of cloud technologies will be still key to enable scalable and autonomic IoT infrastructure spanning from cloud to edge (or across edges). Cloud-native approaches have been proved to work effectively also in distributed scenarios and to enable role out and automation of IoT services in the cloud- edge continuum. Evolutions of these technologies will be key to allow IoT to scale at the edge and across multiple infrastructure providers.
- **Hardware & Sensors:** the role of edge computing clearly depends on the evolution of hardware. Edge nodes are requested to run AI and machine learning tasks that so far were only possible in cloud infrastructures, while dealing with other constraints such as energy capacity. The latest developments in microprocessor architectures and ongoing research (e.g. neuromorphic computing) should provide novel computing capacities able to support AI tasks not possible today at a lower energy footprint than today. The increasing number of deployed sensors will also impact IoT sustainability, thus demanding for - not only more energy efficient sensors - but as well more bio-compatible ones.
- **Cybersecurity:** the move from a centralized infrastructure to a distributed and decentralized one, - while clearly reducing the need to move data to third party infrastructures - it increases the complexity of security management and increases the potential surface of attack of the infrastructure. It is expected that security and privacy technologies will evolve to scale in a decentralized deployment and to increase their resiliency to novel mechanisms of attack that may compromise edges.

- **Big Data and Edge Computing:** IoT systems typically generate heterogeneous data from distributed sensors. The overhead of data with lack of relational databases to handle them results in semi-structured and non-structured forms as well (e.g., Surveillance cameras). Data integrity becomes paramount in big-data security and edge computing applications.

5. IoT Security

The Internet of Things (IoT) systems are prototypical examples of cyber-physical systems wherein there is a tight coupling between physical and cyber subsystems with unknown and/or challenging environmental interactions. Manufacturers and industries are producing an incredible variety and volume of IoT devices. Deviating from traditional Information Technology (IT) devices, IoT is typically cyber-physical in nature with environmental interactions. In addition, they may depend on other devices or systems for their operations. Typically designed using embedded devices having limited memory and processing power, but working in a networked environment for complex systems makes them vulnerable to attacks. While their capabilities to enable applications that abstractly engaged the scientist's attention is often exacerbated; security concerns are subtly ignored. Nevertheless, Nextgen services and applications require tight security mechanisms and therefore, the devices should guarantee devices' security, trust, and reliability. Therefore, the IoT system manufacturers should ensure adequate security, and gain the users' trust. For example, even in non-engineering applications such as banking over mobile phones, 4G and 5G device security becomes paramount. Moreover, the platforms on which such services run could range from a laptop, mobile phones, PDA, and even a small device.

The IoT devices are used by diverse customers: industries, laboratories, individuals, households, and so on. Unfortunately, the IoT devices lack security features to help mitigate cyber-security risks. Consequently, customers/solution architects need to identify cyber-security risks and implement mechanisms/algorithms to address cyber risks. The result is many cyber devices are not secured properly and the devices could be easily compromised.

Selecting the right cyber-security risk management for the device is paramount; but requires addressing certain challenges specific to the IoT systems, they are:

- Limited memory and processing power of the embedded processors/devices used in the IoT. With increasing data rates, complexity of security mechanisms, and devices with scarce processing resources. Metrics such as Million Instructions Per Second (MIPS).
- Communication and computing constraints imposed by certain embedded devices.
- Limited power requirements of these devices, device management, and at times inability to replenish power in these devices.
- The IoT systems deployed in extreme environments subjected to shocks, vibrations, lighting, power supply fluctuations, etc.
- Cost-sensitivity of the devices towards high performance security algorithms.
- Cloud-connectivity, edge computing, different networking layers (application, network, & physical), and computing platforms.
- Presence of heterogeneous devices with various communication protocols from different vendors presents challenges in terms of interoperability and cyber-security on the other.
- Computing on edge and real-time data requirements with security is a demanding task on resource constrained devices.
- Performing complex tasks such as video processing in real-time while guaranteeing security on single board computers or SoCs is complex as well.

These unique features of the IoT impose new challenges for secured design and attention should be paid to these aspects during design. Else, it could lead to costly design upgrades and the worst-case system performance could be compromised as well.

As the number of IoT devices increases, it becomes more difficult to manage and limit unauthorized access or malevolent behaviour. According to studies, 98% of all IoT device network communication is in plaintext, exposing sensitive data on the network and enabling attackers to listen to unencrypted network traffic, grab personal or secret information, and

profit from it on the dark web. Imaging devices are used in 51% of healthcare risks, interrupting care and allowing attackers to acquire patient data stored on these devices. IoT and IT assets are intermingled in 72% of healthcare VLANs, allowing malware to spread from users' laptops to vulnerable IoT devices on the same network. Attackers use their vulnerabilities to conduct a wide range of criminal activities, including compromising privacy, converting devices into a botnet, initiating DoS / DDoS assaults, infecting with ransomware, mining crypto currencies, and so on. Figure 4 depicts a variety of security ideas that may be incorporated into the IoT data flow.

Six principles of IoT Cyber Security across the stack

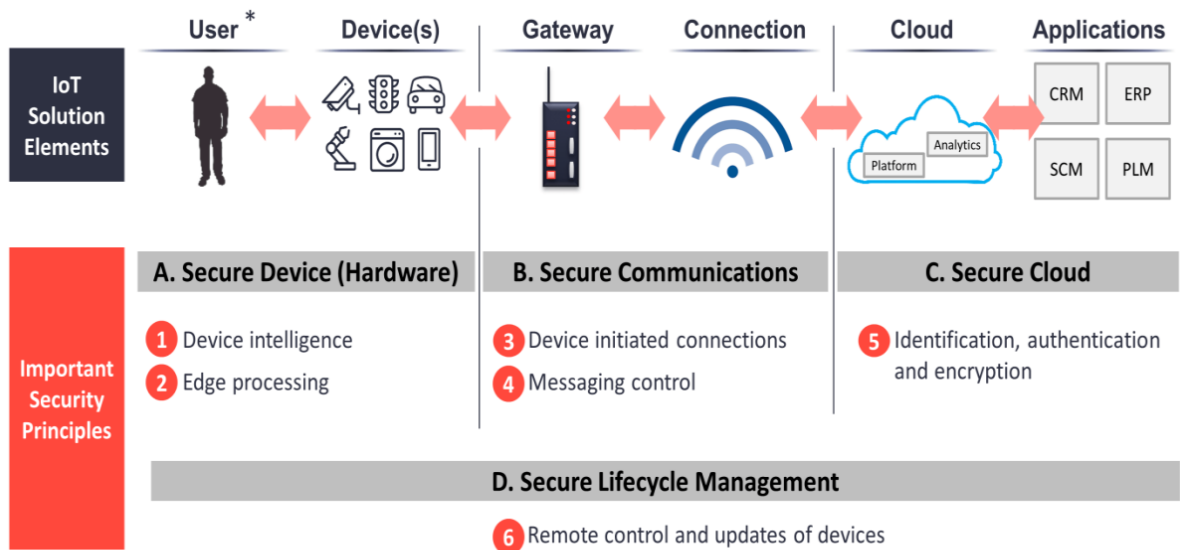


Figure 4: Principle of IoT Security [3]

To analyze the security of IoT devices, we should first understand the many components involved, then identify what kind of security vulnerabilities may influence each component and investigate each of them. There are three major categories of Internet of Things device infrastructure: Embedded system, Computer software & applications, and Wired/Wireless communication system.

5.1. Need for Security in the IoT Ecosystem

The global total of cyber-attacks targeting the IoT will approach 112 million events by 2022. Statistic has risen significantly in recent years, with the number of detected cases climbing from roughly 32 million in 2018. The occurrence of malware events associated to the IoT increased by 87 percent year on year in the most recent recorded year [4]. Figure 5 illustrates the annual number of IoT malware attacks. Malware attacks on IoT and operational technology (OT) devices have surged 400% from 2022 to 2023. The analysis, which examined over 3,00,000 thwarted assaults on IoT devices over a six-month period, revealed the tenacity of cyber threat actors, demonstrating that attackers are mostly targeting older vulnerabilities. With a 961 percent increase in IoT malware attacks, the education sector suffered a significant increase.

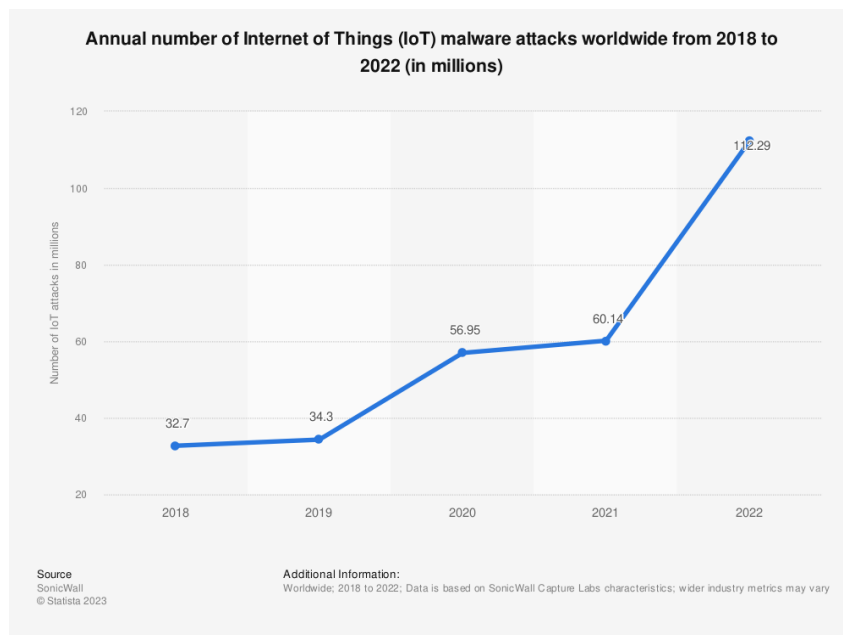


Figure 5: IoT malware attacks statistics [4]

Weak enforcement of IoT device manufacturer security standards, along with the development of shadow IoT devices at the business level, poses a huge threat to worldwide organizations. Threat actors frequently target 'unmanaged and unpatched' devices to get an early foothold in the environment. 'Mirai' and 'Gafgyt' malware families continue to account for 66% of attack payloads, building botnets from infected

IoT devices that are subsequently used to perform Distributed Denial-of-Service (DDoS) attacks against valuable enterprises. 3D printers, geolocation trackers, industrial control devices, car multimedia systems, data gathering terminals, and payment terminals sent most signals over digital networks, accounting for roughly 52% of IoT device traffic.

The abundance of personal data kept on their networks has made educational institutions particularly appealing targets, leaving students and administrations vulnerable. Furthermore, the survey revealed that the United States is a primary target for IoT malware authors, with 96% of all IoT malware disseminated from compromised IoT devices in the country. Mexico had the greatest infections, accounting for 46% of all IoT malware infections [5].

The security of the IoT encompasses a diverse array of concerns due to the multitude of components that contribute to the overall functioning of an IoT system. The components encompass interconnected devices, gateways, platforms for overseeing IoT implementations, and data-consuming endpoints in the form of applications and visualization displays. The process of gathering and transmitting data among these components through various exclusive and standardized communication protocols exemplifies the various combinations and intricacies inherent in IoT systems.

Consequently, the matter of IoT security is more complex than merely implementing encryption for data transmission between a sensor and an application. The complexity of deployed IoT systems is significantly higher. Numerous instances encompass a substantial quantity of interconnected devices and sensors. As an illustrative case, communication pathways can consist of numerous hops through intermediate gateways. In addition to addressing technological considerations, the safe remote management of field devices also entails resolving operational challenges. Additionally, there can be prerequisites for integrating equipment various suppliers provide and their respective technical standards. Figure 6 depicted the comprehensive security at various layers of IoT.

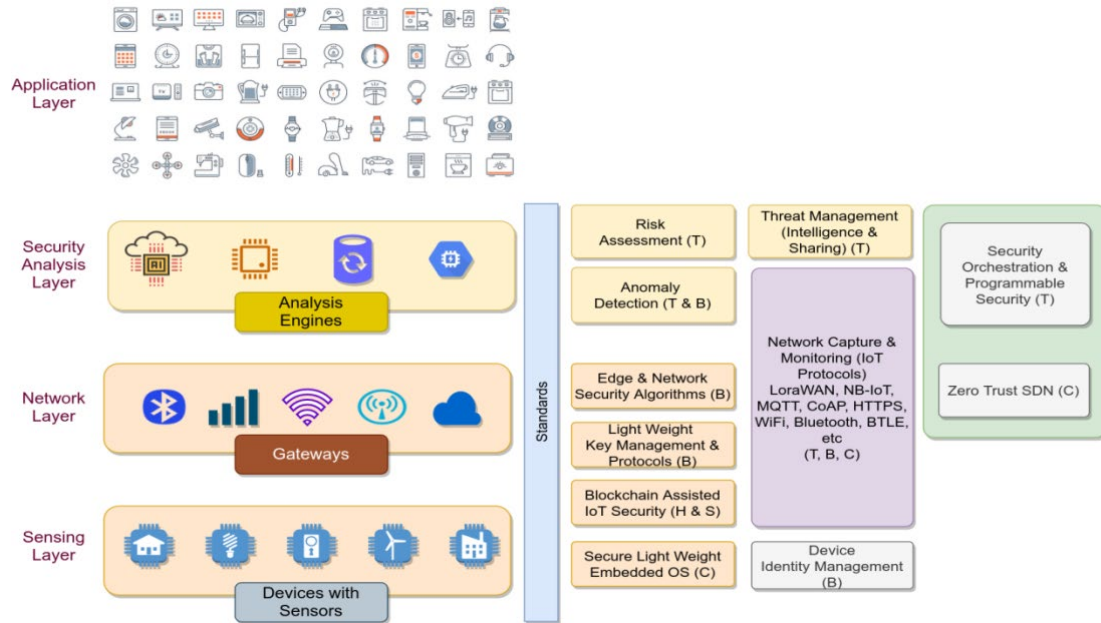


Figure 6: Security at various layers in IoT

5.2. Hardware Level Security

Device identification and spoofing are one of the fundamental requirements/attacks on the IoT. Device spoofing happens when security breaches through a lower end device on a shared IoT network. Device cloning, device related timing attacks, node capture attack, side-channel attack, device substitution, non-repudiation, and firmware level attacks. Device identification related attacks are quite common in the IoT and identifying these attacks are quite challenging. Spoofing is an active attack where the attacker already has access to the system and stays inactive initially to observe the data traffic. Upon sensing an anomaly, identity spoof node starts sending signals to neighbour nodes. Two common ways of securing IoT applications against device spoofing is through: localization and channel-based detection. Approaches such as received signal strength (RSS), AOA (angle of arrival), and TDoA (Time Difference of Arrival) are used. Tamper attack involves physical tampering of the IoT device to make the circuit behave differently from required behavior.

Any IoT architecture relies on the "Device" component. The term "device" in this context refers to any hardware device that is involved in architecture. For example, the

"gateway" and the "operating device" are typically included in most smart home equipment. The gateway serves as a central hub for the other devices, whereas the "operating device" is the device that does the actual activity or monitors via sensors, depending on its purpose. The vulnerabilities in "device" will be any vulnerability found in an embedded device. Some of the examples we'll start with include serial port connection leading to root access and the ability to retrieve firmware from the flash. In coming posts, we will go through these in further detail after covering the device part.

Radio communication is an essential component of any IoT device. By radio communication, we simply mean any communication that occurs between machine to machine. Wi-Fi, BLE, LoRa, NB-IoT, Zigbee, Z Wave, 6LoWPAN, and Cellular are some of the communication protocols that are commonly utilized in IoT ecosystem. To effectively conduct an IoT device pentest, we will need to examine and map the complete attack surface for that specific device. Assessing an IoT device attack surface is like mapping a web attack surface, but there are many more components involved. The steps for mapping the attack surface of an IoT device are as follows:

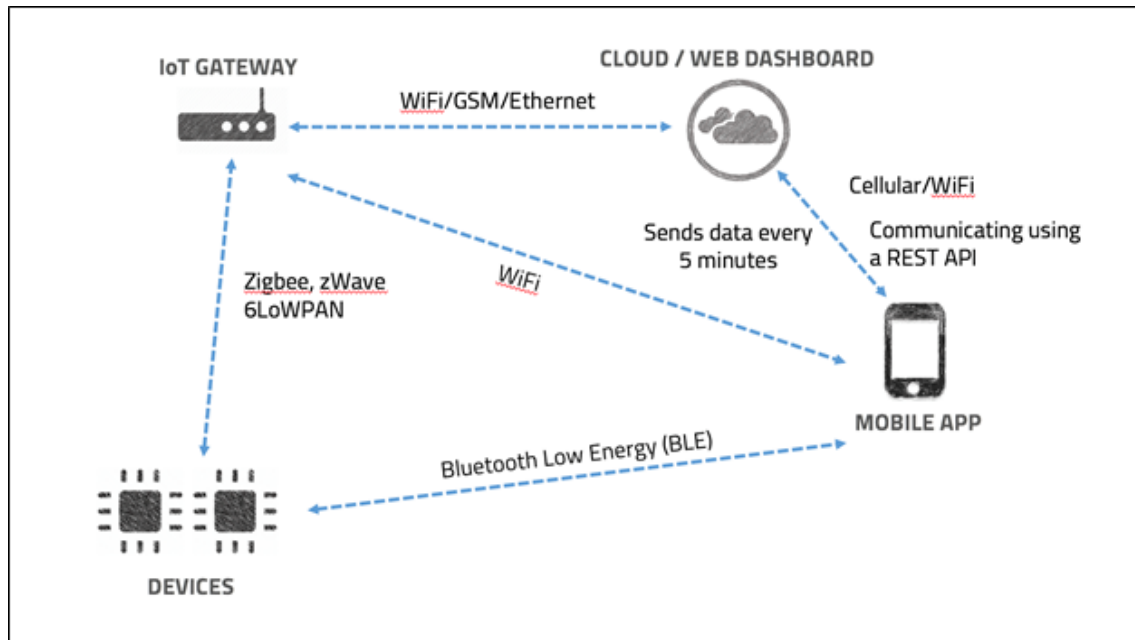


Figure 7: Communication Pathways of Devices

Step 1: Understanding the complete IoT device architecture is the initial step in Attack Surface mapping. It would necessitate a thorough examination of all product manuals, paperwork, material on the vendor's website, and any extra information obtained from any other source.

Step 2: Create an architecture diagram for the specified device, detailing each component mentioned in Figure 7. If it is a radio communication between two devices, draw a dotted line and indicate the type of communication protocol utilized. Mark the architectural diagram with the type of API used if the application communicates with the cloud to send and receive data using an API.

Step 3: Consider yourself an attacker once you've completed the whole architecture diagram. What strategies would you employ and what type of information would you try to obtain if you had to attack a specific component? In a spreadsheet, list all the specific test cases for each component.

Gateway is a kind of IoT device. Gateways are components that connect low-end edge devices to high-end devices, services, and/or applications. Therefore, a compromised gateway influences the reliability and performance of the system significantly. Attacks on gateway may also include data related attacks that tend to affect the data integrity. Malicious code injection, stealthy attack, routing attack, ICMP flooding, cache attack, wormhole attack, SLAAC (stateless Address Auto configuration Attack), HSRP (Hot Standby Router Protocol), RIPv2, EIGRP, and OSPF are common types of attacks on the gateway. Many attacks on the gateway could also be driven by applications and could compromise the entire networked system.

5.3. Network Level Security

A host of attacks happens in an IoT system in the network related aspects. IP spoofing, DNS spoofing, replay attack, man-in-the middle attack, eaves-dropping attack, unauthorized tag attacks, spear-phishing attack, Sybil attacks, Sinkhole attack, Denial of Service, stealthy attack, bias injection attack and others. Networks are the most

vulnerable component in an IoT system. Other attacks include Hello flood attack, sewage pool attack, blitch attack, flash crowd attack, and others.

- The replay attack refers to spoofing of one or more nodes wherein they share their identity and they harm system confidentiality. Two widely used ways to handle replay attack are: timestamping and prevention using nonce option.
- Man-in-the-middle attack is widely found in wireless sensor networks, here the attacker eavesdrops the network and gains access to the confidential data. Initially, the attacker sniffs the network, but once enough knowledge on the system is available, personification happens. The attack usually happens over network packets.
- Unauthorized access to tags is an integral part of the IoT. Many systems using RFID, NFC, and other communication protocols are commonplace for this attack. The attacker changes the whole node as a result malicious node is part of the network and could easily gather information and could be source of further attacks.

An attacker can see the key exchange/transport packets of the wireless protocol by sniffing the traffic between the Gateway and low-end devices. As a result, the designer should safely implement these key exchange/transport packets in accordance with the protocol. Any insecure implementation may reveal the key (or set of keys) to the attacker, compromising the confidentiality of the communication.

DDOS are a form of cyber-attack wherein the perpetrator latches to a single connection point and uses this channel to send multiple messages or requests for information. This could easily happen in IoT systems wherein there are vulnerable nodes such as networked thermostats, monitor etc. Setting up firewall is considered a good solution for DDoS attacks. ICMP flooding is a common gateway attack. It is a common DoS attack in which an attacker aims to overwhelm a target IoT device with echo requests thereby causing flooding of packet requests over network leading to the device being inaccessible over the network.

5.4.Application-Level Security

Examining the application allows us to identify the various attacks. These attacks include DNS amplification, insecure http, frame jacking, SQL injection, cross-site scripting, LDAP injection. Buffer overflow, etc. The application layer decides the real-time performance of the IoT device/system and communicates with external entities such as cloud and web interfaces. An IoT device's Software and Cloud component includes Device firmware, Web application dashboard, Mobile application used to control, configure, and monitor the devices. Each of the components has some special vulnerabilities. Unauthorized access is quite common in application-level attacks. Some of the common application-level attacks are explained here:

- A malicious code is the generic term for various viruses, worms, and trojan horses. They harm the system with an attacker injecting a malicious code into the system to disrupt the whole network thereby compromising the whole network.
- Insecure software and/or firmware: As IoT devices are connected to web, cloud, and other systems, the backend software becomes core point of attacks. To guarantee security, software should be upgraded regularly. The data formats e.g., XML, CBOR, JSON etc., need to be tested prior to deployment because of these issues. Hence proper software testing of all associated components is essential.
- SQL injection attack: Common application layer attack in which the attacker attempts to boost data flow via SQL interfaces, erase a database, and many other things.

While there are various ways to characterize IoT cyber-security levels, perception, network, and application are elaborated on in depth. There are several potential solutions for dealing with IoT cyber-security. Anomaly detection for detecting device spoofing and malware, developing machine learning and deep-learning models for security assessment from data, using existing recommendations from standards and other Pen tests suggested in various standards, network related security assessment, dynamic whitelisting,

cryptography-based solutions, and steganography-based solutions are common approaches.

5.5.Security in IoT Operating System

IoT operating systems are specialist software platforms designed to handle and manage a wide range of devices that are interconnected inside the Internet of Things (IoT) ecosystem. These operating systems are intended to address the special issues given by the diverse and frequently resource-constrained nature of IoT devices. The operating systems are specifically intended to fulfil the unique needs of IoT devices, including capabilities and characteristics that enable successful communication, data processing, and networking inside the IoT ecosystem.

The inherent lightweight architecture of IoT operating systems is critical due to the limited processing power and memory capacity of many IoT devices. These operating systems (OSs) have been intended to be resource efficient, allowing them to run on microcontrollers and CPUs with restricted capabilities. Furthermore, these devices provide real-time functionality, ensuring that IoT devices respond quickly to various sensors and events. Contiki-NG, Zephyr, FreeRTOS, RIOT, mbedOS, and TinyOS are examples of popular IoT operating systems. These operating systems include a wide range of tools and libraries designed to make the process of designing IoT applications easier. These OSs make IoT devices easier to adopt in a variety of domains, including smart home appliances, wearable devices, industrial automation, and smart cities. As a result, they are a key component of the IoT infrastructure.

IoT operating systems, in essence, serve an important role within the IoT ecosystem due to their adaptability to the specific demands of IoT devices. These operating systems offer lightweight and real-time functionality, allowing for efficient communication and data processing. OS with specialized capabilities have a significant impact on the advancement and adoption of IoT devices across a wide range of applications. Following security measures needs to be considered in terms of security in IoT Operating System:

- To protect data in transit, use secure communication protocols such as CoAPs (Constrained Application Protocol over DTLS), MQTT with TLS, or LwM2M with DTLS.
- Select appropriate cryptographic algorithms for encryption and authentication while keeping IoT device resource limits in mind.
- Implement secure boot mechanisms to ensure that only authenticated and authorized firmware is loaded into the device.
- To protect against vulnerabilities, enable secure firmware upgrades by signing and validating firmware images before installation.
- Design access control policies to grant devices and users access to certain resources or to conduct specific tasks.

Security management in IoT OS demands the execution of a complete approach that includes technical measures, adherence to best practices, and continual vigilance. It is critical to assess the specific security requirements and vulnerabilities of your IoT application and then implement appropriate remedies. It is critical to keep in mind that the level of security required will vary based on the sensitivity of the data and the potential implications of security breaches in your IoT deployment.

6. National and International IoT Security Standards

Several nations and international organizations have actively pursued the development of national or regional standards and guidelines for IoT security. The goal of these standards is to create a complete structure for safeguarding IoT devices, networks, and systems in order to ensure data confidentiality, device integrity, and overall ecosystem security. These standards and recommendations may range in scope and applicability, but they are connected by common principles such as data protection, encryption, device identity and authentication, secure upgrades, and vulnerability management. It is critical to recognize that the world of IoT security standards is always changing, with the possible creation of new standards and rules. To improve the security of IoT deployments, organizations and manufacturers should

stay up to date on the most recent breakthroughs in IoT security standards and ensure adherence to the appropriate requirements in their countries. Several examples of national and regional initiatives and standards relevant to IoT security from various nations are presented below:

- The United States is a country located in North America. The U.S. National Institute of Standards and Technology (NIST) has established an all-encompassing framework aimed at enhancing cybersecurity in many sectors, encompassing the IoT. The IoT Cybersecurity Improvement Act, enacted in 2020, mandates that federal agencies must adhere to designated cybersecurity protocols while utilizing IoT devices within government infrastructures.
- The European Union (EU) is a supranational organization consisting of 27 member states located primarily in Europe. The European Union has implemented the EU Cybersecurity Act, which encompasses a comprehensive structure for the certification of security measures pertaining to IoT devices and systems. One aspect of this endeavor involves the establishment of a comprehensive framework for cybersecurity certification within the European context. The General Data Protection Regulation (GDPR) is a comprehensive legal framework that governs the protection and processing of personal data inside the European Union (EU) and the European Economic Area (EEA). Although the General Data Protection Regulation (GDPR) is not exclusively targeted at the IoT, it enforces stringent regulations around data protection and privacy for all organizations, including those involved in processing IoT data.
- The United Kingdom is a sovereign country located off the northwestern coast of mainland Europe. The United Kingdom government has just released a voluntary code of practice aimed at enhancing the security of consumer IoT devices. Code of practice is intended to be followed by manufacturers, service providers, and merchants to ensure the implementation of improved security measures.
- Germany is a country located in Central Europe. The BSI IoT Security Recommendations provide guidelines and suggestions for enhancing the security of

IoT devices. The German Federal Office for Information Security (BSI) has recently issued a set of guidelines pertaining to the security of IoT devices. These recommendations encompass a wide range of considerations related to the security of such devices.

- Singapore is a sovereign city-state and island country located in Southeast Asia. The Cyber Security Agency of Singapore (CSA) has formulated a comprehensive handbook on IoT cybersecurity, encompassing a range of best practices and suggestions aimed at fortifying the security of IoT devices and systems.
- China is a country located in East Asia. The Ministry of Industry and Information Technology (MIIT) in China has just released a set of IoT security guidelines. These standards provide a comprehensive framework that establishes the necessary security requirements for both IoT devices and services.
- Japan is a country located in East Asia. The Ministry of Economy, Trade, and Industry (METI) in Japan has recently published recommendations pertaining to the security of IoT systems. These guidelines aim to safeguard the confidentiality, integrity, and privacy of such systems.
- Australia is a country located in the southern hemisphere, specifically in the region of Oceania. The Australian government has released a Code of Practice for the Internet of Things (IoT), offering recommendations on the implementation of security measures for IoT devices and data protection.

Following are the different standards used for IoT Security (Devices):

International Standards

ISO/IEC 30141 [6]	<p>IoT (Internet of Things) - Reference Architecture</p> <p>The standard provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs, and industry best practices. It uses a top-down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model, deriving a high-level system-based reference with subsequent dissection of that model into five architecture views from different perspectives.</p>
ISO/IEC27402 [7]	<p>Cybersecurity - IoT security and privacy - Device baseline requirements</p> <p>Provides baseline requirements for IoT devices to support security and privacy controls.</p>
ISO/IEC 27400 [8]	<p>Cybersecurity — IoT security and privacy — Guidelines</p> <p>Provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.</p>
ISO/IEC DIS 27403 [9]	<p>Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics</p> <p>Provides guidelines to analyze security and privacy risks and identifies controls that need to be implemented in IoT-domotics systems.</p>
ISO/IEC 20924 [10]	<p>Information Technology Internet of Things (IoT) - Definition and Vocabulary</p> <p>Provides a definition of Internet of Things along with a set of terms and definitions. This document is a terminology foundation for the Internet of Things.</p>

NISTIR 8228 [11]	<p>Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks</p> <p>This document contains the following:</p> <ul style="list-style-type: none"> • Cybersecurity and Privacy Risk Considerations • Challenges with cybersecurity and privacy risk mitigation for IoT Devices • Recommendations for Addressing Cybersecurity and Privacy Risk Mitigation Challenges for IoT Devices
NIST IR 8425 [12]	<p>Profile of the IoT Core Baseline for Consumer IoT Products</p> <p>The consumer profile of NIST’s IoT core baseline and identifies cybersecurity capabilities commonly needed for the consumer IoT sector (i.e., IoT products for home or personal use). It can also be a starting point for small businesses to consider in the purchase of IoT products. The consumer profile was developed as part of NIST’s response to Executive Order 14028 and was initially published in Recommended Criteria for Cybersecurity Labelling for Consumer Internet of Things (IoT) Products. The consumer profile capabilities are phrased as cybersecurity outcomes that are intended to apply to the entire IoT product. This document also discusses the foundations to develop the recommended consumer profile and related considerations. NIST reviewed a landscape of relevant source documents to inform the consumer profile and engaged with stakeholders across a year-long effort to develop the recommendations.</p>
NIST SP 800 53 [13]	<p>Security and Privacy Controls for Information Systems and Organizations</p>

<p>NISTIR 8259 Series [14]</p>	<p>The NISTIR 8259 series of reports provides guidance for manufacturers and their supporting third parties as they conceive, design, develop, test, sell, and support IoT devices across their spectrum of customers.</p> <p>NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities</p> <p>NISTIR 8259A: Core Device Cybersecurity Capability Baseline</p> <p>NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline</p> <p>NISTIR 8259C (DRAFT): Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline</p>
<p>NISTIR 8267 [15]</p>	<p>Security Review of Consumer Home IoT Products</p> <p>Presents the results of a project that conducted a technical review of security features in different categories of consumer home Internet-of-Things (IoT) devices. The categories of IoT devices included smart light bulbs, security lights, security cameras, doorbells, plugs, thermostats, and televisions. The purpose of the project was to better understand security capabilities of these IoT devices and to inform general recommendations for manufacturers for improving the security of consumer home IoT devices. This report provides those recommendations, along with observations of IoT devices' security features, to indicate current practices and how these current practices could be improved.</p>
<p>ITU-T SG</p>	<p>ITU-T (International Telecommunication Union) Special Group</p> <p>SG 17 - IoT Security [16]</p> <p>SG 20 - IoT and its applications in Smart Cities & communities [17]</p>

<p>SP 800-213 Series [18]</p>	<p>IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements</p> <p>SP 800-213 explains the role of IoT devices as elements of federal systems and provides guidance for addressing the unique risks such devices can present. SP 800-213 is complemented by SP 800-213A, the IoT Device Cybersecurity Requirements Catalog, a collection of technical and non-technical cybersecurity controls defining a broad range of IoT device capabilities and supporting non-technical actions that an agency can apply in documenting their IoT cybersecurity requirements. SP 800-213A includes mappings to SP 800-53 and NIST Cybersecurity Framework controls for traceability to RMF guidance, and an IoT cybersecurity profile based on the RMF low-impact baseline control set in SP 800-53B (this profile was original published as draft NISTIR 8269D)</p>
<p>ETSI EN 303645 [19]</p>	<p>The standard defines the Cyber-security guidelines for the consumer internet of Things. Cyber-security provisions for IoT recommended are:</p> <ol style="list-style-type: none"> 1. No Universal passwords 2. Implement means to manage vulnerability reports. 3. Keep software updated. 4. Securely store sensitive security parameters. 5. Communicate securely. 6. Minimize exposed attack surfaces. 7. Ensure software integrity. 8. Personal data security 9. Resilience to outages. 10. Examine telemetry data. 11. User data deletion. 12. Easy device installation and maintenance

	<p>13. Input data validation</p> <p>Further, some data protection aspects are recommended in the standard.</p>
IoTSTF	<p>Internet of Things Security Foundation</p> <p>The Internet of Things Security Foundation (IoTSF) is a not-for-profit, global membership association working to make the connected world ever-more secure.</p> <ul style="list-style-type: none"> • IoT Security Assurance Framework [20] • Vulnerability Disclosure Best Practice Guidelines [21] • Secure Design Best Practice Guides [22]
IEC 62443 [23]	<p>The standard deals with secure industrial automation and control systems throughout their life cycle. It currently includes nine standards, technical reports, and technical specifications. IEC 62443 addresses not only the technology that compromises a control system, but also the work processes, countermeasures, and employees. The standard takes a holistic approach. The IEC 62443 standards is organized into four parts:</p> <p>Part 1: Covers topic common to the entire series.</p> <p>Part 2: Policies and Procedures:</p> <p>Focuses on methods and processes associated with Industrial Automation and Control System (IACS) security.</p> <p>2-1: Establishing IACS security program</p> <p>2-2: Patch management in the IACS environment</p> <p>2-3: Security program requirements for IACS service providers</p> <p>Part 3: System Requirements</p> <p>3-1: Security technologies for IACS</p>

	<p>3-2: Security risk assessment for system design</p> <p>3-3: System security requirements and security levels</p> <p>Part 4: Components and Requirements</p> <p>4-1: Secure product development lifecycle requirements</p> <p>4-2: Technical security requirements for IACS components</p>
EuroSmart	EuroSmart is a trade organization involved in the digital security field and aims to build open-source standard for IoT devices.
Other Initiatives	Other standards are provided by IoT Standard Foundation, IASME, European Network and Information Security Agency (ENISA), and Institute of Electrical and Electronics Engineers (IEEE)

Indian Standards

TEC 31318 [24]	<p>Code of Practice for Securing Consumer Internet of Things (IoT)</p> <p>Telecommunication Engineering Center developed this document which contains following:</p> <ul style="list-style-type: none"> • Guidelines for securing Consumer IoT • Data protection provisions for consumer IoT
LITD 17 (19140,19141,19143) [25]	<p>Internet of Things Security & Privacy</p> <p>Part 1: Overview</p> <p>This document provides concepts, reference models and risks of Internet of Things.</p> <p>Part 2: Controls and Requirements</p> <p>This document lists out controls, assurance levels and requirements for security and privacy of IoT.</p> <p>Part 3: Assessment and Evaluation</p> <p>This document provides the compliance process, approach and methodology for assessment and evaluation of Internet of Things with compliance checklist.</p>

IoT Policy Document [26]	Government of India had formulated a Draft IoT Policy with a vision to develop connected and smart IoT based system for our country's economy, society, environment, and global needs. This Policy launched a Smart City project, with a plan of developing 100 smart cities in the country
TEC-TR-SN-M2M-009 [27]	Examines the principles and approaches for enabling security in IoT / M2M solution domain and prepares the recommendations for way forward
IS 18004 : Part 1 [28]	IoT Reference Architecture: for the Concept Model, IoT Reference Models and IoT Deployment Views
ITU-T Y.3056 (02/21) [29]	Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems for its comprehensive treatment of low-cost approach to IoT Security based on operator trust
TEC 31328: 2023 [30]	Security by Design for IoT Device Manufacturers
ITU-T Y.3052 [31]	Trust provisioning in ICT infrastructures and services consists of a set of processes that include gathering data from entities and producing trust information by evaluating all aspects of trust to support the decision making of entities when establishing trust relationships with other entities.
TEC 31188 [32]	The project on National Trust Centre for IoT Devices, its Architecture and Design, together with the ongoing work to realize an implementation that works with the TEC MTCTE portal
TEC 93009 [33]	The Mandatory Testing and Certification regime and its impact on the security controls in the IoT space
ITU-T Y.4500.3 [34]	oneM2M – Security solutions, provides specifications for machine to machine (M2M) security, and privacy protection.

National standards typically focus on meeting the specific criteria of different countries, whereas international standards promote global compatibility and collaboration. Both national and international standards play pivotal roles in the regulation and standardization of IoT security products and their solutions. These will help to accomplish the IoT security in various domains.

7. IoT Application domains and Security Issues

The Internet of Things (IoT) is a rapidly growing network of networked devices and systems that gather, exchange, and use data to improve ease and efficiency in our daily lives. The IoT has the potential to change various industries/applications such as Smart Home Automation, Smart Agriculture, Smart Cities and many more; yet it also poses a slew of security challenges. The growing proliferation of IoT devices has increased the opportunity for malicious actors to exploit flaws and launch attacks within the IoT ecosystem.

7.1.Smart Home

Smart home automation applications provide unrivalled convenience and control, but they also pose security threats. Understanding these threats and executing mitigation techniques are critical for ensuring your smart home's privacy and security. Attackers intercepting data sent between devices and potentially acquiring sensitive information. To mitigate, utilize encryption protocols such as WPA3 for Wi-Fi networks, employ end-to-end encryption for device connection, and regularly examine device permissions and settings for data sharing. Malicious software infecting smart home devices is another attack that could lead to data breaches or device takeover by cybercriminals. To combat, users should install trusted security software on their network and devices, routinely update device firmware to patch vulnerabilities, and avoid side-loading apps on devices.

7.2.Smart City

Smart cities utilize technological breakthroughs to increase the quality of urban living; nonetheless, they are challenged with a broad variety of IoT security concerns. IoT Cyberattacks on essential infrastructure have been seen, notably targeting key services such as electrical grids, water supply, and transportation networks. To address the deployment of effective network security and intrusion detection systems, it is required to engage in periodic testing and updating of vital infrastructure systems. Additionally, the construction of contingency plans and backups is vital to ensure the continuity of services. In a possible scenario, an attacker successfully performs a hijacking operation, obtaining unauthorized access and effectively acquiring control of a targeted device. As the attacker did not make

significant changes to the device's basic functions, identifying such attacks can be challenging. In the context of a smart city, an attacker might possibly exploit a compromised smart traffic system to launch ransomware attacks on Traffic Management Systems.

7.3.Smart Agriculture

Smart agriculture, also known as precision agriculture or agtech, is a revolutionary farming practice that uses cutting-edge technologies, data analytics, and IoT devices to improve and optimize agricultural practices. Smart agriculture is a practice that blends real-time monitoring, automation, and data-driven decision-making to empower farmers in improving crop yields, reducing resource waste, encouraging sustainability, and effectively meeting the world's increasing food demand. It will enable farmers to be more efficient and environmentally responsible.

A masquerade attack is the use of fake identity to gain unauthorized access to secret information about a farm's operational activities. Identifying such attacks may be difficult because of attackers' fraudulent activity, which mimics the actions of ordinary users. To counteract masquerade attacks, various strategies are used. Common preventative techniques include employing a variety of approaches to improve the security of a system's authentication process. It is recommended to use machine learning methodology for detecting attackers through analyzing their movement patterns within a file system.

7.4.Smart Grid

A smart grid is an advanced electrical infrastructure that uses digital technology, bidirectional communication, and real-time data analysis to increase the efficiency, dependability, and environmental friendliness of power generation, distribution, and consumption. The incorporation of modern advancements into the traditional power grid facilitates the establishment of a smart grid, which in turn improves energy resource management, allows for the incorporation of renewable energy sources, reduces power outages, and empowers consumers by giving them more control and information. Finally, advancement provides the groundwork for a more resilient and responsive electrical system.

False Data Injection Attack (FDIA) is commonly regarded as one of the most serious and harmful threats against smart grid systems. An unauthorized user gains access to the system and manipulates the sensor data in a way that introduces undetectable errors into the estimate of state variables and scheduling decisions in the context of Fault Detection, Isolation, and Accommodation. In comparison to accessing the communication channel, accessing the physical network directly is substantially more challenging. This attack is distinguished by the attacker's deliberate targeting of the communication network and communication channel in order to manipulate sensor readings. Detecting these types of attacks is a difficult and time-consuming task. To counteract this type of attack, it is advised that an architecture based on Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) methodologies be presented. The architecture should seek to detect the location of False Data Injection Attacks (FDIA) in real time.

7.5. Healthcare

The significance of security in the healthcare sector is of utmost importance due to a multitude of factors and outcomes that could endanger human life. Healthcare organizations are responsible for managing confidential and highly personal data, which frequently pertains to critical and perhaps life-saving matters. Further, information regarding comorbidity, multi-pharmacy, treatment plans, and even expenditures could provide data that could be important to healthcare industry. The failure to adequately safeguard this data can result in significant repercussions for individuals, institutions, and society at large. There exist several fundamental justifications for the necessity of security measures within the healthcare industry.

- The preservation of patient privacy is a critical concern within the healthcare industry, as healthcare providers are responsible for the collection and storage of extensive and sensitive patient data. This data encompasses medical records, personal information, treatment plans, clinical intervention, lifestyle interventions, and billing details. The preservation of data privacy is not solely a legal obligation, as exemplified by the HIPAA regulations in the United States, but also a fundamental ethical responsibility.

- Medical identity theft is a significant concern as healthcare records hold considerable value for individuals engaged in identity theft activities. Insufficient security measures for patient data may result in its unauthorized acquisition, enabling fraudulent actions such as the illicit acquisition of medical services or prescription drugs using counterfeit identities.
- The provision of quality care at healthcare institutions can be compromised by security breaches, leading to disruptions in regular operations and therefore impacting the timeliness and overall quality of patient care. The occurrence of delays or disruptions in the provision of patient treatment can lead to severe, sometimes life-threatening outcomes.
- The healthcare industry is required to adhere to a multitude of rules and standards, including the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Adherence to these standards is obligatory, and the implementation of security measures is required in order to fulfil legal obligations.
- The maintenance of data integrity is crucial in the healthcare setting as it ensures that patient data is both accurate and dependable, hence facilitating effective medical decision-making. Security measures play a crucial role in maintaining the integrity and accuracy of data, hence mitigating the risk of errors in diagnoses and treatment.
- The sharing of patient data between various providers and systems is of utmost importance in the context of a more integrated healthcare ecosystem. Ensuring the security of data during its transmission between entities is of paramount importance.
- The utilization of smart medical devices and IoT technology in the healthcare sector is progressively growing, hence presenting novel security challenges. The exploitation of vulnerabilities in these devices has the potential to cause harm to patients or undermine the security of critical data.
- Ransomware poses a significant threat to the healthcare industry, as it is frequently targeted by such assaults. The act of encrypting patient data by cybercriminals and

subsequently demanding a ransom can result in the disruption of operations and pose a significant threat to the lives of patients.

- Healthcare institutions frequently engage in research and clinical trials, which involve the systematic investigation and evaluation of medical interventions and practices. Ensuring the safeguarding of research data is crucial not only to uphold scientific integrity but also to uphold the safety of patients and the privacy of data.
- The security of electronic prescription systems is crucial in ensuring the prevention of unauthorized access or tampering with medicine orders, as such actions might potentially lead to significant implications for patient well-being.
- Accountability and audit trails are essential security features that provide the tracking of individuals who have accessed patient records and the corresponding timestamps. The establishment of accountability is of utmost significance in ensuring adherence to regulatory requirements and facilitating inquiries pertaining to security breaches.
- The preservation of public trust is a critical imperative for healthcare organizations. The occurrence of a data breach or privacy violation has the potential to negatively impact an organization's reputation and undermine the trust of both patients and the wider community.
- The financial consequences of data breaches can be substantial, since they may incur legal fines, patient litigation, and expenses related to repair efforts and the preservation of reputation.
- The implementation of security measures can effectively reduce the likelihood of inadvertent data breaches resulting from human mistake, including instances such as the transmission of sensitive information to an unintended recipient or succumbing to phishing attempts.
- Availability is a critical component in healthcare security with confidentiality and integrity. Since device availability is critical for securing human lives and personal data, guaranteeing it amidst security concerns is challenging.

- As for data, restricted data-sharing or preferential sharing is unavailable for IoT security. It is important for enabling the user to identify the data that could be shared without compromising the personal data.
- In the context of a device, integrity refers to the trait of being dependable and trustworthy. In general, the loss of device integrity can be ascribed to either functionality or data corruption. An such example is the intentional exploitation of medical devices via a reprogramming attack. The consequences of this type of hacking can vary greatly depending on the clinical application of the device. Taking control of devices that are closely linked to the human body, such as implantable medical devices or pumps, has the potential to result in death or physical harm. The detection of slight cognitive manipulation, such as the manipulation of neurostimulation devices, may provide additional difficulties.
- A Denial-of-Service (DoS) attack has the potential to be used to deplete the battery of an Implantable Medical Device (IMD). To mitigate the attacks against IMDs, it is recommended that proprietary protocols be used to restrict unauthorised access. Furthermore, it is advised that the firmware of these devices be continually updated within a secure environment.

Considering the significant implications and potential ramifications involved, it is imperative for healthcare establishments to allocate resources towards the implementation of comprehensive security protocols. These measures encompass data encryption, access controls, security training, and periodic security evaluations. The primary objective is to safeguard patient data and guarantee the welfare and security of individuals seeking medical attention.

7.6.Industrial IoT

The importance of security in the context of the Industrial Internet of Things (IIoT) cannot be overstated due to the nature of IIoT, which entails the interconnection of industrial equipment, sensors, and control systems with the internet and other networks for the purpose of enhancing operational efficiency and productivity. The preservation of security in IIoT

systems is of utmost importance to avert disturbances, safeguard confidential information, and uphold the integrity of industrial processes.

- Operational integrity refers to the ability of IIoT systems to effectively manage and oversee crucial industrial operations. Security breaches have the potential to cause significant disruptions to many operational processes, resulting in adverse consequences such as delays in production, damage to equipment, and financial losses.
- Safety is a critical concern in industries that heavily rely on IIoT technology, including manufacturing, energy, and healthcare sectors. Inadequately secured Industrial IIoT systems have the potential to result in accidents, injuries, or even fatalities.
- The generation and processing of a substantial volume of sensitive operational and performance data is facilitated by the IIoT. Ensuring the protection of this data is crucial to uphold corporate competitiveness and mitigate the occurrence of data breaches.
- Process efficiency is a primary objective of the IIoT, which seeks to enhance and streamline industrial operations through optimization and automation. The use of security measures is important to guarantee the effectiveness and dependability of these procedures.
- Intellectual property (IP) is a crucial aspect of numerous IIoT solutions, as they often incorporate exclusive technologies, designs, and operational processes. The protection of intellectual property rights necessitates the critical task of securing these assets.
- Supply chain security in the context of IIoT frequently depends on the utilization of networked devices and components sourced from diverse sources. The implementation of security measures is necessary to mitigate vulnerabilities that may be introduced at any stage within the supply chain.
- Industries are required to adhere to a multitude of rules and standards, including those established by esteemed organizations such as the International Society of

Automation (ISA) and the National Institute of Standards and Technology (NIST). The adherence to these requirements frequently requires the implementation of strong security protocols.

- The increased interconnectivity of IIoT systems with networks and the internet has rendered them susceptible to cyberattacks. Adversarial entities possess the capability to exploit inherent weaknesses inside IIoT systems, thereby inflicting harm, disrupting normal operations, or pilfering confidential data.
- Quality control is a crucial aspect of IIoT systems since they play a significant role in ensuring the maintenance of product quality and consistency. The occurrence of a security breach has the potential to lead to the manifestation of product flaws or inconsistencies.
- Loss prevention refers to the implementation of security measures aimed at safeguarding valuable assets and commodities, with a particular focus on businesses such as warehousing and logistics, where the risk of theft and tampering is prevalent.
- The IIoT has the potential to exert substantial environmental effects. The implementation of security measures is necessary in order to efficiently regulate and monitor systems, hence mitigating any environmental damage.
- Public safety is a paramount concern in various sectors, including transportation, utilities, and healthcare, where IIoT solutions are occasionally employed. A potential compromise in the security of these systems may lead to disturbances that have an impact on the safety and welfare of the public.
- Legacy systems refer to industrial systems that have been in existence for an extended period and may not have been originally developed with contemporary security practices in consideration. The use of security solutions aimed at retrofitting can effectively safeguard these historical systems against contemporary threats.
- The evaluation of vendors and suppliers plays a critical role in ensuring the adherence to security requirements and the right assessment of IIoT devices and solutions, thereby effectively limiting potential risks.

- The Man in the Middle attack refers to the hypothetical scenario in which an attacker puts themselves between an industrial IoT endpoint device and the cloud or centralized network, the attacker pretends to be the device and deceitfully transfers data. The main threat occurs when communication from an endpoint device has the capacity to modify production data or exert control over a field-deployed product. In the context of the bolt manufacturing industries, consider a hypothetical situation in which an attacker assumes the identity of an industrial IoT sensor and intentionally provides incorrect data. This false behaviour may result in the recalibration or modification of manufacturing procedures within the production equipment. As a result of this nefarious action, the production of defective bolts may occur unintentionally. A hardware-based security solution can establish a root of trust, allowing the central network to determine the authenticity of the source of information with certainty, distinguishing between a real endpoint device and an unauthorized entity.

In essence, the implementation of security measures in the context of IIoT is imperative to safeguard individuals, valuable resources, sensitive information, and vital industrial operations. The growing evolution and interconnectivity of IIoT technologies necessitate the implementation of strong security measures to guarantee the secure and uninterrupted functioning of industrial processes and systems.

The importance of security in Industrial automation cannot be overstated, especially in industrial and manufacturing environments where automation technologies are integral to the control and optimization of diverse processes. There are several fundamental justifications for the necessity of security in industrial automation.

- The issue of safety arises in the context of industrial automation systems, which are responsible for the control of machinery and processes that possess inherent risks if not adequately safeguarded. The maintenance of security in these systems is of utmost importance to mitigate the occurrence of accidents, injuries, and potentially deadly incidents.
- The generation and reliance on enormous volumes of data by automation systems is a significant aspect of data protection. The dataset may encompass confidential designs,

operational data, and information of a sensitive nature. Ensuring the protection of data is of utmost importance to sustain corporate competitiveness and mitigate the risk of data breaches.

- Automation systems play a crucial role in numerous industries, contributing to the overall business continuity. The occurrence of any disturbance or breach in these systems has the potential to cause substantial periods of inactivity, financial losses, and harm to a company's standing. The implementation of security measures is necessary to guarantee the uninterrupted operation of a firm.
- The utilization of automation plays a crucial role in enhancing the efficiency of manufacturers and enterprises in the production of goods, hence contributing to the safeguarding and promotion of intellectual property. The intellectual property encompassing blueprints, drawings, and proprietary techniques employed in automation holds significant value. The implementation of security measures is crucial to safeguard these valuable assets.
- The prevention of unauthorized access is of utmost importance in automation systems, as such access can lead to detrimental consequences such as data manipulation, sabotage, or theft. Security measures, such as access controls and authentication protocols, serve the purpose of mitigating the risk of unauthorized individuals gaining unauthorized control over these systems.
- Compliance with laws is a crucial aspect for numerous businesses, as they are required to adhere to specific standards and guidelines established by reputable organizations such as the International Society of Automation (ISA) and the National Institute of Standards and Technology (NIST). Adherence to these laws is frequently mandated by law and entails the implementation of strong security protocols.
- Supply chain security is a critical concern in the context of automation, as it frequently entails the utilization of networked devices and components sourced from several providers. The establishment of robust security measures is of utmost

importance to mitigate the potential risks that may arise at any stage within the supply chain.

- The increased interconnectivity of automation systems with networks and the internet has rendered them susceptible to cyberattacks, necessitating the implementation of protective measures. Malicious entities have the capability to exploit vulnerabilities present in automation systems with the intention of inflicting harm, disrupting operational processes, or pilfering confidential data.
- Quality control encompasses several automation systems that are tasked with the crucial responsibility of upholding the standards and uniformity of products. The occurrence of a security breach has the potential to lead to the manifestation of product flaws or inconsistencies.
- Loss prevention refers to the implementation of security measures aimed at safeguarding valuable assets and materials, with a particular focus on businesses such as warehousing and logistics, to prevent theft and tampering.
- The implementation of automation technology can provide substantial environmental consequences. The implementation of security measures is necessary in order to efficiently manage and monitor systems, with the ultimate goal of minimizing any potential negative impact on the environment.
- The use of automation systems in vital sectors such as transport and utilities is occasionally observed in the context of public safety. A potential compromise in the security of these systems has the potential to cause disruptions that have implications for the safety and overall welfare of the public.
- Legacy systems refer to automation systems that have been in operation for an extended period and may not have been originally developed with contemporary security practices in consideration. The implementation of security measures can be crucial in safeguarding historical systems from contemporary dangers.

Latency can cause frequent transitions between cloud and local processors in the automobile, potentially introducing errors in its operation. Manipulation of safety-critical

systems is one such type of attack. It happens when an automobile receives faulty essential real-time data, which can cause the vehicle to stall or cause an accident. Vulnerability scanners and Extended Detection and Response (EDR) systems are two potential options to explore. Scanners are computerized programmes that routinely check endpoints, servers, networks, and apps to uncover any security holes that hostile actors could exploit. The EDR system is intended to collect and analyze detailed data on many stages of the data supply chain, such as the vehicle, network, and backend servers. This enables a high level of detection and investigative capability.

7.7.Security in Automotive

The Automotive IoT Security Lifecycle and the broader Cybersecurity Lifecycle have evolved in response to the growing integration of IoT technology in vehicles and the critical concerns surrounding the safety and security of connected and autonomous cars. The automotive industry and the broader cybersecurity community recognized the importance of understanding the evolving threat landscape, which involved understanding the specific vulnerabilities posed by IoT integration in connected vehicles and the tactics and motives of cyber adversaries.

Both lifecycles moved into the planning and risk assessment phase, where stakeholders assessed potential vulnerabilities and threats, recognizing the implications of security breaches on vehicle safety and the impact of data breaches, financial losses, and reputational damage in the broader cybersecurity arena.

Security measures were implemented in both domains, with automotive IoT implementing secure boot processes, encryption protocols, intrusion detection systems, and secure over-the-air (OTA) updates, while the broader cybersecurity field implemented solutions such as firewalls, antivirus software, intrusion detection and prevention systems, and encryption protocols.

Compliance and regulations played a role in both lifecycles, with regulatory bodies and standards addressing automotive IoT security and data protection. Both domains adapted to emerging threats by developing advanced security measures, threat intelligence sharing, and the incorporation of artificial intelligence and machine learning.

Collaboration and information sharing within and across industries were vital in addressing global threats.

		Vehicle Life-Cycle			
		Design	Development	Production	Post-Production
Cyber Security Life-Cycle	Cyber Risk Mangement	Identify and manage cyber risks to certain veicle types across the supply chain			
		Ensure testing of security of systems			
		React to new and evolving cyber threats and vulnerabilities			
	Security by Design	Ensure security in the detail design phase, test information, and collect evidence across the full supply chain			
		Analyze cyber threats and create a risk treatment plan			
		Build security into system design and contain known vulnerabilities in (re)used HW/SW 1 components		Protect the integrity of HW/SW components from suppliers.	
		Test the security of HW/SW 1 components (e.g., with vulnerability scans, pen testing, code analysis)		Protect access to the software servers and the flashing process received from suppliers	
	Detect and respond to security incidents				Monitor and respond to cyberattacks on vehicles and their ecosystem
	Secure Software updates	Ensure full traceability of software versions and vehicle configuration along the vehicle lifecycle			
					Identify target vehicles for updates and assess impact to certified systems and compatibility with vehicle configuration
			Provide software updates without impacting safety and security impact		

Figure 8: Interdependency between Cyber Security Lifecycle and Vehicle Lifecycle

As cybersecurity continues to evolve, it is imperative that automotive IoT security matures, adapts, evolves, and improves in tandem [35, 36]. A symbiotic relationship between these two domains is illustrated in Figure 8, highlighting the interdependence that underscores the necessity for to advance in lockstep. Both domains must advance together to ensure the safety and security of connected and autonomous vehicles, as they become increasingly prevalent in the digital age.

With the automotive sector extending towards technology centric systems, several new technologies like electric vehicles, autonomous functionality, connected vehicles, etc., are being considered. The software definition of these vehicles is in constant change and requires frequent configurations and updates. Moreover, it is moving to the paradigm of AI and ML. Cybersecurity therefore becomes the most important aspect of these systems because human lives are at stake in the vehicle. The automotive therefore becomes the new attack surface. Developing cybersecurity at the hardware, communication and software levels of the vehicle is essential to ensure the safety of commuters. Better techniques are required for ensuring that the operational and functional stringencies of the

vehicle are maintained, especially with security in place, requiring new innovations towards security provisioning.

Connected Vehicles (V2X) and Drones: The connected vehicles and UAV/Drones are going to be on the rise in the future. Connectivity like vehicle-to-vehicle and swarm will create a new dimension of threats due to mobility and collaborative operation. The nature of attack and the degree of harm caused to the infrastructure may be difficult to accurately predict and deploy the protection mechanism.

Software Defined Vehicles: Software Defined Vehicles are the new focus of the automotive sector from a long-term perspective. With growing demand for higher computation and communication in vehicles, the software definition of the vehicle requires considerable change. Research thought is being played out towards self-driving vehicles and this is shaping up with several industries entering this space. Providing cybersecurity for self-driving vehicles becomes an essential part of the future. The long-term vision of the automobile business is currently shifting towards the concentration on Software Defined Vehicles, with particular attention being given to cybersecurity measures. The increasing need for enhanced computational and communication capabilities in automobiles necessitates significant modifications to the software definition of the vehicle. Research interest is currently focused on self-driving vehicles, and this field is witnessing significant involvement from several sectors. Ensuring cybersecurity measures for self-driving vehicles emerges as a crucial aspect of the forthcoming era.

In the automotive industry, the use of communication technology is reliant on radiofrequency waves for the transmission and reception of data in our existing cellular networks, WiFi systems, and upcoming 6G networks. In scenarios where wireless communication capabilities are pushed to their maximum thresholds, such as densely populated crossroads, there exists a significant vulnerability to interference. The phenomenon of network saturation may provide challenges for connected vehicles in situations where many vehicles attempt to connect to a shared network simultaneously. Likewise, wireless connections may experience limitations in their functionality when

confronted with poor network signals or obstructions, such as in underground tunnels or locations with uneven terrain.

These elements may contribute to accidents because of heightened latency in data transmission among cars, as even a minimal delay might have significant consequences. Hence, it appears that the dependability of wireless connectivity utilizing radiofrequency technology is not totally sufficient for the purposes of traffic control and safety. An alternative to radio frequency (RF) technology is the use of Light Fidelity (Li-Fi) for the purpose of smart traffic control. By employing Li-Fi, communication between numerous vehicles and various components of the road infrastructure, including traffic lights, signals, signboards, and vehicles themselves, may be facilitated in a rapid and uninterrupted manner. The implementation of Li-Fi technology has the potential to significantly enhance safety measures within the traffic system. Li-Fi technology has the potential to revolutionize the automotive industry by facilitating the integration of advanced safety systems, improving infotainment capabilities, and upgrading passenger experiences in connected automobiles.

Li-Fi differs from cellular network technology in that it utilizes light as a medium for data transmission between two devices. Li-Fi technology offers rapid data transmission rates and is characterized by enhanced security features. The incorporation of Li-Fi technology inside the automotive ecosystem holds the potential to facilitate the development of autonomous driving, intelligent traffic management, and uninterrupted vehicle-to-cloud connectivity. The potential of connected cars appears promising, with Li-Fi technology playing a pivotal role in advancing driving safety, efficiency, and overall user engagement.

A major sales segment is the after-market products that cater to sales of product after the vehicle is deployed on roads. These products are manufactured by different vendors from different countries with various standards. Guaranteeing the security of these products is critical and quite cumbersome as well. Establishing security mechanisms for aftermarket products is essential for the automotive segment.

There exist numerous IoT application domains apart from the above mentioned, and these domains are expected to continue growing as improvements in technology progress. In essence, the implementation of security measures in automation is imperative to safeguard individuals, resources, information, and vital operations. The rising advancement and interconnectedness of automation technologies necessitate the implementation of sophisticated security measures to guarantee the smooth and secure functioning of diverse industries and businesses.

8. IoT Security: Future and Trends

The IoT working groups and the Cybersecurity consortium have mapped relevant initiatives and tools in this context of the IoT ecosystem. This section builds on the IoT R&D priorities, presenting an overview of the most important challenges and topics in the IoT domain from a security, privacy, and policy perspective. As for many other new technologies, understanding how to increase trust toward the IoT by end-users requires a multidisciplinary approach. In this respect, data privacy and safety should be regulated from an ecosystem approach and managed in this complexity of changing roles, various types of data, and data reuse.

In terms of IoT security, experts observed that the new data paradigm, in which less data is stored in data centres and more data is distributed pervasively closer to the user "at the edge," presents new issues for cybersecurity. It was also observed that securing IoT applications is not just about protecting personal data and business data, it is about protecting people as individuals, as citizens, and as users of services.

Forecasting the exact condition of IoT security in the next decade poses a formidable task due to the rapid evolution of technology and the constant emergence of novel dangers and advancements. Nevertheless, it is possible to formulate informed hypotheses by analyzing prevailing patterns and anticipated advancements in alternative technologies. Over the course of the next decade, it is anticipated that the field of IoT security will see significant advancements and transformations in various aspects. Some of the major/critical areas and topics under each area identified for research and large innovation potential in the near-to-long term are: oneM2M, eSIM Cellular-IoT, Lightweight Cryptography, Blockchain and Distributed Ledger Technology and many others.

The trajectory of IoT security will be influenced by the dynamic technological environment, the escalating prevalence of IoT devices, and the advancing complexity of cyber risks. The forthcoming discourse will outline many significant trends and advancements that are anticipated to influence the trajectory of IoT security in the future. The integration of machine learning and artificial intelligence will have a substantial impact on the enhancement of security measures inside the IoT domain. These technologies have the capability to be employed for the purpose of detecting threats in real-time, identifying anomalies, and executing automated reactions to security incidents.

Fine-grained privacy refers to the ability to exert exact control and protect the privacy of individuals' data and actions inside the context of networked devices. This concept focuses on giving users complete control over information sharing, including the selection of recipients and the implementation of specified circumstances. In the context of fine-grained privacy in the IoT, the deployment of advanced access control, encryption, and anonymization techniques enables users to create and enforce their privacy choices at a granular level, even down to individual data points. These techniques ensure that personal information is only exchanged with permitted entities, reducing the dangers associated with privacy breaches or unauthorized data use in the increasingly linked IoT world.

The Zero Trust Architecture, characterized by the fundamental principle that no entity, regardless of its location within or outside the network, should be inherently trusted, is expected to gain further prominence in the realm of IoT security. The methodology implements stringent access constraints and ongoing monitoring. The utilization of blockchain technology has the potential to bolster the security of IoT devices through the provision of tamper-resistant record-keeping and device authentication mechanisms. The utilization of blockchain technology can contribute to the preservation of data integrity and the verification of device IDs.

The adoption of security-by-design concepts is expected to rise among IoT device manufacturers, as they incorporate security safeguards into the early stages of device development. The consideration of security will no longer be relegated to a secondary position. The increasing prevalence of data processing and decision-making at the periphery

of IoT networks necessitates the implementation of security measures at the edge to safeguard data and devices against local threats. Standardization plays a crucial role in the advancement and widespread implementation of secure IoT systems. The ongoing efforts to establish and embrace global IoT security standards and best practices facilitate the task of organizations in safeguarding their IoT installations.

Enhanced identity and access management systems will play a crucial role in regulating the authorization of individuals to access IoT devices and associated data. The prevalence of biometric authentication and multi-factor authentication is expected to increase in the future. In the realm of IoT device management, organizations will prioritize the implementation of robust protocols for secure device onboarding, continuous monitoring, and end-of-life procedures. This strategic approach aims to mitigate potential security risks that may arise at any stage of the device's lifecycle. Governments and regulatory entities will persist in implementing and revising legislation pertaining to the security of IoT systems. The adherence to these regulations will be of utmost importance for parties involved in the IoT.

Organizations are expected to allocate resources towards ensuring the comprehensive security of the IoT ecosystem, encompassing various components such as devices, communication routes, cloud services, and the applications that facilitate the interaction with IoT data. The adoption of risk assessment and threat intelligence will likely become a prevailing approach in the field of IoT security. This proactive strategy involves evaluating potential hazards associated with IoT devices and leveraging threat information to predict and effectively address emerging attacks.

Supply chain security is expected to become a focal point for organizations, as they prioritize safeguarding their IoT supply chain against potential vulnerabilities that may arise from third-party components and vendors. Education and Awareness for Users: End-users and employees will be provided with training and resources aimed at enhancing their comprehension of security concerns associated with the IoT and promoting the adoption of best practices for safe use. The utilization of device profiling and behavioral analytics entails the examination of the behavior shown by IoT devices, as well as the analysis of data flows,

with the objective of identifying atypical patterns. This approach is employed to promptly identify and address potential security concerns.

The rise of quantum computing necessitates the development of cryptographic algorithms that are resistant to quantum attacks to safeguard IoT data. **Enhanced Collaboration and Information Sharing:** The augmentation of collaborative efforts across manufacturers, organizations, and cybersecurity specialists would facilitate the exchange of threat intelligence and optimal strategies, so enabling a more efficient response to the security problems posed by the IoT. The inclusion of quantum sensors in the IoT has the potential to yield significant effects. Quantum sensors possess the remarkable capability to measure temperature, pressure, and magnetic fields with unparalleled precision, rendering them highly suitable for deployment across various sectors, including healthcare, transportation, energy, navigation, and positioning [37].

Threat modelling is an essential practice in the context of Industrial Control Systems (ICS) and the IoT for identifying and managing security risks that might harm critical infrastructure and industrial operations. The methodical assessment of the complete ICS infrastructure, including IoT devices, sensors, communication protocols, and human interactions, to identify vulnerabilities and potential attack vectors is known as threat modelling. Organizations can build specialized security measures, prioritize risk mitigation methods, and strengthen the resilience of their ICS and IoT ecosystems by considering diverse risks such as insider threats, external attacks, and supply chain vulnerabilities.

Furthermore, ICS-specific threat modelling considers the inherent operating requirements and limits of industrial contexts, such as the need for real-time response and reliability. It considers threats that could have serious implications, such as process disruptions, safety dangers, or environmental impacts, and ensures that security measures are in line with the ICS's specific aims and functions. As threats to ICS and IoT systems increase, threat modelling remains an important tool for protecting critical infrastructure and ensuring operational continuity.

The future development of intrusion detection in the context of the IoT is expected to be influenced by emerging patterns such as the increasing use of ML and AI for anomaly

detection, the development of intrusion detection systems that are optimized for IoT devices in terms of their lightweight nature and efficient resource utilization, and the emergence of edge-based intrusion detection techniques aimed at masked intrusion detection. As the IoT grows and evolves, intrusion detection systems should adapt and address the distinct issues that arise from the widespread adoption of interconnected devices, the increasing complexity of IoT ecosystems, and the increasing complexity of cyber threats. As a result, it is envisaged that there will be an increase in the development of proactive and autonomous intrusion detection systems, as well as improvements in interoperability with other security methods. To properly safeguard the IoT environment, there will also be an emphasis on the development of privacy-aware detection technologies.

Forensic tools in IoT are specialized instruments and software applications meant to examine and analyze IoT devices and the data they generate in cases of IoT security incidents, breaches, or other types of unauthorized access. These technologies assist digital forensic experts in extracting, examining, and interpreting evidence from IoT devices and networks, assisting in incident response and security assessments. These tools may be used in analysis of the Device hardware or software. Some of the tools are Device emulators, Bug analyzers, Network packet Analyzers, IoT Vulnerability Assessment and Penetration Testing (VAPT) tools, Event logging tools etc. These forensic tools for IoT may be built in as per standards(NIST's Computer Forensic Tool Testing (CFTT) program, etc.) with the evolving IoT ecosystem and the increasingly sophisticated nature of security threats in consideration.

Several significant trends in network monitoring on the IoT are likely to emerge in the future. The developments include the rise of artificial intelligence-powered analytics for monitoring and predicting network behaviour in real time. Furthermore, progress has been made in the development of network protocols and standards specifically adapted for the IoT, with the goal of improving data interoperability and visibility. Furthermore, there is a growing emphasis on edge computing and distributed monitoring solutions that attempt to reduce latency and improve network performance. Furthermore, with the increasing scale of IoT implementations, network monitoring tools must improve their scalability, efficiency, and cost-effectiveness to keep up with the ever-expanding IoT environment. Furthermore, it is critical to prioritize security as a top priority. It emphasizes the monitoring of unusual activity

and potential hazards within IoT networks in order to ensure the validity and dependability of IoT applications and services.

In the future years, the trajectory of IoT security will be defined by a continual desire for innovation and adaptation to effectively tackle an ever-changing spectrum of threats. It is imperative for both organizations and people to adopt a proactive approach, acquire knowledge about optimal security measures, and maintain a constant state of alertness to safeguard their IoT devices and networks. The significance of IoT security is poised to escalate as the integration of IoT permeates many domains of our lives and companies.

9. Proposed Roadmap

9.1.Ongoing Activities

The projects listed below are now underway at various Indian government organizations such as CDAC (at different centres), SETS, ERNET, and others.

- 1) We are now engaged in the development of a national facility dedicated to the testing, evaluation, and certification of Internet of Things (IoT) devices and embedded systems, with the goal of ensuring security assurance. The primary aim of the project is to develop a National Facility for Testing, Evaluation, and Certification of IoT Devices and Embedded Systems. It will encompass the following key functions:

The establishment of a Security Testing and Evaluation Lab for IoT Devices and Embedded Systems is recommended, which assess the susceptibilities of Consumer Electronics (CE) Commercial Off-The-Shelf (COTS) IoT devices and Embedded Systems. Our examination will concentrate on several device elements, including hardware, embedded software, on-board and external communication interfaces, and wireless radios.

The objective of the study is to develop, evaluate, and identify tools that can be used to conduct audits, assess the security of IoT devices and embedded systems, and ultimately provide end-user security assurance. The project aims to develop National Standards and

investigate potential contributions to the Protection Profile (PP) for IoT Devices and Embedded Systems.

The objective is to establish a laboratory dedicated to doing side-channel attack and analysis research, equipped with the necessary instruments and infrastructure. In the realm of capacity building, our objective is to support national efforts by organizing training sessions and certificate programmes focused on two key areas: security testing of IoT devices and the development of secure IoT devices and applications. These programmes are designed to benefit various stakeholders, including industry professionals and other interested parties.

The outcome of the project is to produce a comprehensive paper or book that focuses on the evaluation of IoT device security. This resource will include in-depth techniques, case studies, and instructions for various technologies. Additionally, the implementation of a Security Testing and Evaluation Lab for the Internet of Things (STeALTh) is proposed. The proposed initiative is the establishment of a laboratory known as the Side Channel Attack and Analysis Lab for Embedded Systems and IoT (SCALE-IT). Capacity building can be achieved through the implementation of workshops and short-term training programmes.

- 2) The project is to design SDN and NFV based Network Service Delivery Platform for Enterprise and Service Providers. It includes development of network service delivery platform including Network Function Virtualization Infrastructure (VNFI) comprising COTS Hardware platform and Hypervisor, Virtual Network Functions (VNF) and Network Service Orchestrator. It also includes implementation and Delivery of Network services/Network Functions through the platform including SDWAN, DHCP/DNS, Web Proxy, Routing/Switching and Firewall Functions. The major outcome of the work is to come up with SDN enabled Virtual Network Function Platform, SDWAN and Network Service Orchestrator along with field trials.
- 3) The security of the IoT can be enhanced by using the Firmware Lightweight Trusted Platform Module (FLTPM) in conjunction with a TLS-like protocol that utilizes lightweight algorithms. Study focuses on the design and development of a Firmware

Lightweight Trusted Platform Module (FLTPM) using lightweight algorithms. The objective is to deploy a TLS-like protocol utilizing lightweight techniques throughout IoT edge networks, encompassing both the edge devices and IoT Gateway. To conduct comprehensive assessments of IoT edge network security, it is necessary to establish a dedicated security test laboratory. This laboratory will be specifically designed to evaluate the security measures used inside IoT edge networks, utilizing the OneM2M compliant Interoperable Platform as a testing framework.

The primary goal is to enhance the efficiency of cryptographic solutions specifically developed for IoT devices. Additionally, the goal is to construct a firmware-based Trusted Platform Module (TPM) that is both adaptable and lightweight. Furthermore, a primary objective is to provide an optimized system that achieves equal Transport Layer Security (TLS) performance. A security testing laboratory is built to assess the security of IoT edge networks, employing an Interoperable Platform that adheres to the OneM2M compliance standards.

- 4) Evaluation Set up for IoT lab at Scientific Analysis Group (SAG) and Formulation of IoT Security Testing Framework. As an integral component of the project, we will undertake the establishment of an IoT Lab utilizing locally developed IoT goods at SAG. Additionally, we will focus on integrating third-party devices into the proposed IoT lab. Furthermore, we will develop a methodology for conducting cyber security testing on networks of IoT devices. Lastly, we will provide practical training on the Indus IoT Kit. The primary objective is to develop an IoT cybersecurity framework and a Vulnerability Assessment and Penetration Testing (VAPT) strategy.

9.2.Short Term (Next 5 years)

9.2.1. IoT Security Sandbox

The IoT security sandbox that has been suggested will offer a means of assessing the device being tested for its vulnerabilities across many levels, including hardware, network, firmware, and application. In the contemporary context, there is a lack of comprehensive security testing for IoT devices in accordance with established

protocols. Furthermore, in the context of the IoT paradigm, security is sometimes given less priority as the focus is on device functionality. This is due to several limitations such as time restrictions for product release, device design considerations including power, memory, communication, and software, as well as the absence of established standards and norms. Consequently, most vendors opt to incorporate their own proprietary security measures, limiting the ability to assess their effectiveness in mitigating potential vulnerabilities. The increasing importance of the IoT has led various application areas, such as Consumer Electronics, Smart Cities, Automotive Industry, Industrial Control Systems, and Healthcare, to integrate IoT devices to enhance their present operations. It is imperative to provide a mechanism for verifying the security status of IoT devices to prevent any potential disruptions to essential infrastructure and processes within the relevant application area.

The primary objective of the IoT Security Sandbox is to establish a comprehensive setting that encompasses a range of tools and protocols for the assessment of security compliance in IoT devices. The sandbox will offer options for assessing four characteristics of the IoT device: Testing the Security of Device Hardware at the Level of Hardware, Evaluation of Security at the Firmware/Software Level and Examination of Security Measures at the Network Level in the IoT ecosystem (as shown in Figure 9).

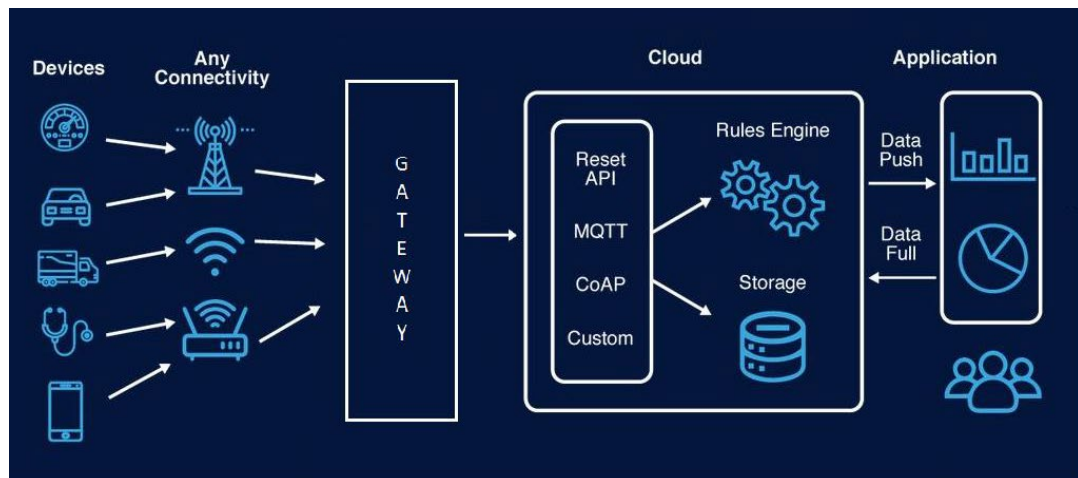


Figure 9: IoT Ecosystem

The topic of interest pertains to the examination of side channel leakage in the context of cryptography. It will suggest the integration of hardware and software security evaluation tools, which are widely accessible in the field of security testing, for the purpose of conducting security evaluations on IoT devices. This integration will involve the development of procedures and methods for performing these tests, which will serve as a repository of knowledge and technological expertise for startups to engage in security evaluation, expand their operations, and carry out ongoing maintenance.

Most technologies utilized to assess security in IoT devices and systems are proprietary. These items are acquired from international suppliers located outside the country, raising concerns about their overall reliability. The development of a comprehensive set of security evaluation tools specific to indigenous contexts is of utmost importance as it will significantly contribute to the establishment and reinforcement of trust within the security evaluation processes conducted in the IoT ecosystem. Furthermore, the IoT ecosystem is characterized by fragmentation, evident in the presence of many device types, protocols, and technologies that constitute the ecosystem. Therefore, it is imperative to prioritize developing and enhancing security evaluation tools and technologies across the entirety of the IoT. the objective will be specifically addressed in the strategic plan.

Regulatory bodies are currently evaluating the inclusion of IoT as a prospective augmentation to the prevailing framework. Nevertheless, because to its fragmented and specialized utilization, the straight application of Common Criteria (CC) to the IoT is not feasible. Instead, it necessitates adaptation to align with the unique requirements of the IoT and its application area. As Common Criteria Recognition Arrangement (CCRA) focuses on adapting the CC standard for the IoT, it is worth considering the development of an ecosystem and the acquisition of skills necessary to implement CC certification in the IoT domain successfully.

9.2.2. eSIM Cellular-IoT

eSIMs are industry-standard digital SIMs that allow enterprises to activate a cellular plan without the need for a physical SIM. One of the key requirements for many IoT use cases is reliable, secure, and extensive wireless connectivity. Cellular networks answer all these requirements, providing a stable, proven, and global service, with a history of strong security. By 2025, GSMA Intelligence forecasts the total number of IoT connections will grow to 25.2 billion and Ericsson projects 5.2 billion cellular IoT connections also by 2025. By the mid-2020s, cellular IoT connections are expected to number more than 60% of mobile handset subscriptions and grow faster [38].

IoT is now rapidly evolving from its roots in monitoring and reporting in the cloud to extensive processing at the network edge, coupled with ‘light’ connectivity to the cloud. The rise of new technologies -Low-power-wide-area-network (LPWAN, Narrowband-IoT (NB-IoT), Massive Machine Type Communications (mMTC), Ultra-Reliable Low-Latency Communication (URLLC) are key enablers in future 5G/6G and beyond networks. A recent GSMA Intelligence survey revealed that 98% of enterprises want an end-to-end security solution that protects data integrity and confidentiality from IoT devices where data is collected to the cloud where it is stored and processed.

Secure, trusted connectivity of IoT nodes shall propel the IoT into the next stage of growth. Trust frameworks and transparency will need to be woven into all IoT layers for our cities to dispel concerns and ensure these new technologies can help our smart cities thrive. The key issue to resolve is how to provide connectivity and zero-touch provisioning cost-effectively, and securely. The eSIM/iSIM technology enables secure identity and large-scale connectivity orchestration among the IoT nodes.

The architecture for the IoT device platform will support GSMA IoT SAFE (IoT SIM Applet for Secure End-2-End Communication), which allows for orchestrating a secure communication channel between the IoT device and mobile network

operator (MNO) remote data centers or in the Cloud infrastructure. The IoT device embeds an eSIM with the IoT SAFE applet (application). As soon as the IoT device is switched on, it is automatically and securely authenticated/provisioned with its IoT applications. Any fraud/spoofed identity (due to theft or tampering) can be detected, and remedial action sequence can be initiated to trace & secure the data on the device. IoT SAFE standardized by the GSMA and a whole ecosystem of major actors in the IoT services space from chipset designers, module providers, (e)SIM providers, connectivity providers, software developers, and IoT cloud service providers are already including support for IoT SAFE in their default offerings (as depicted in Figure 10).

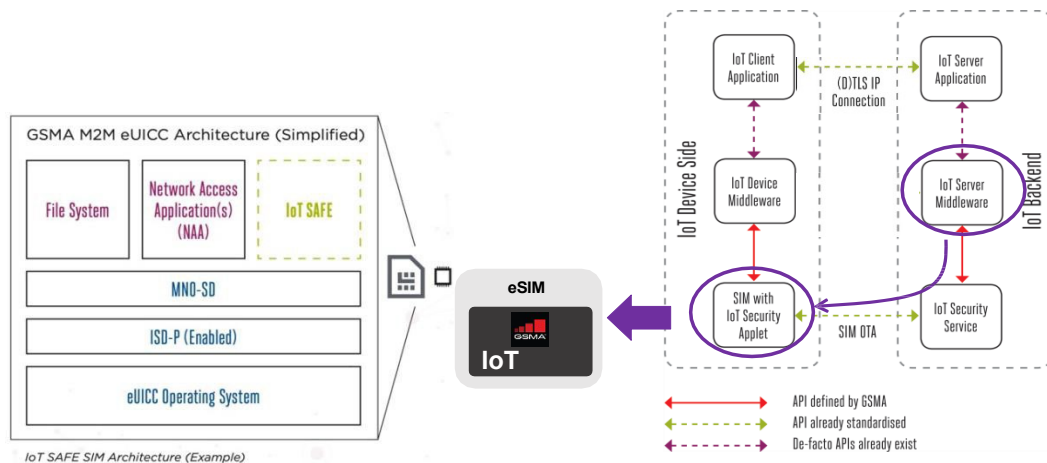


Figure 10: Architecture & working of eSIM

As opposed to physical SIM cards, eSIMs are soldered directly into the device, preventing them from being tampered with or removed to be used fraudulently. As a result, their use in the security of internet-connected devices is significant. In addition to form factor issues, new SIM-based solutions, such as IoT Safe or more complicated domestic counterparts, are broadening the spectrum of security protections available down to the SIM. Furthermore, unlike physical SIMs, eSIMs allow new profiles and agreements to be updated Over The Air (OTA), future-proofing each device's connectivity and removing the need for a physical swap-out of the SIM. As a result, expect to see more enterprises move towards eSIM in coming years.

The new e-SIM is already seeing fast adoption in many markets, especially those related to the Internet of Things. As shown in Figure 11 and Figure 12, adoption is growing in areas like industrial robotics, asset/inventory management, smart grid, and certain personal devices such as smartwatches. The GSMA's Security Accreditation Scheme (SAS) enables mobile operators, regardless of their resources or experience, to assess the security of their UICC and Embedded SIM, suppliers. There is no way to download applications to the Universal Integrated Circuit Card (UICC) without the

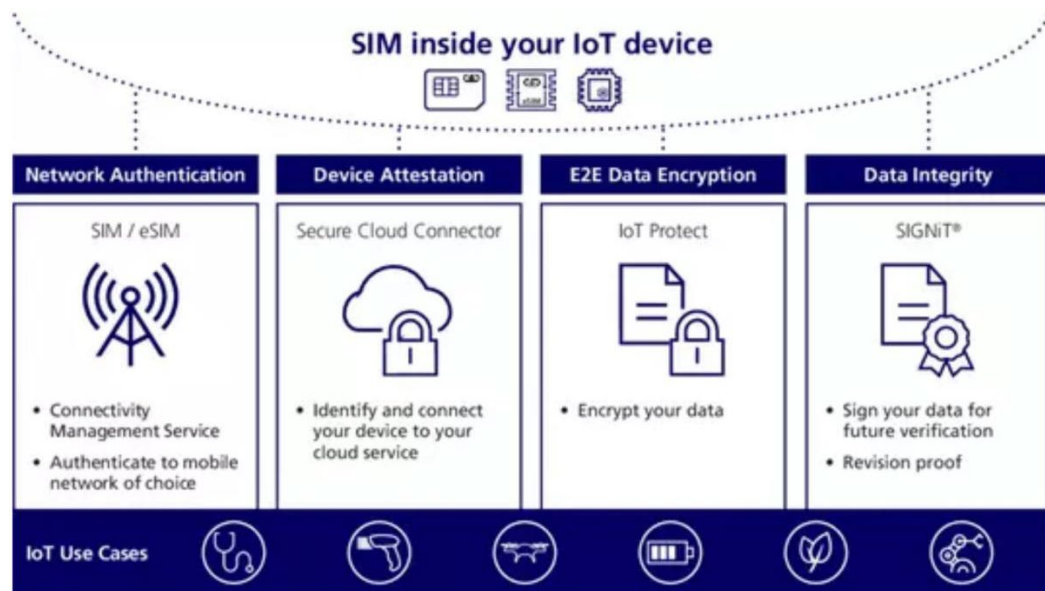


Figure 11: Use cases of eSIM in IoT Devices

Mobile Network Operators' (MNO) consent. At the same time, with so many stakeholders involved (MNO, subscription manager, and eUICC manufacturer), if fraud or a security compromise occurs in an eUICC environment, it may be difficult to quickly identify and fix the root cause because it can occur at so many different levels. Moving from physical SIMs to embedded SIMs will reduce the number that falls into the grey market, making it more difficult to use them for fraudulent purposes.

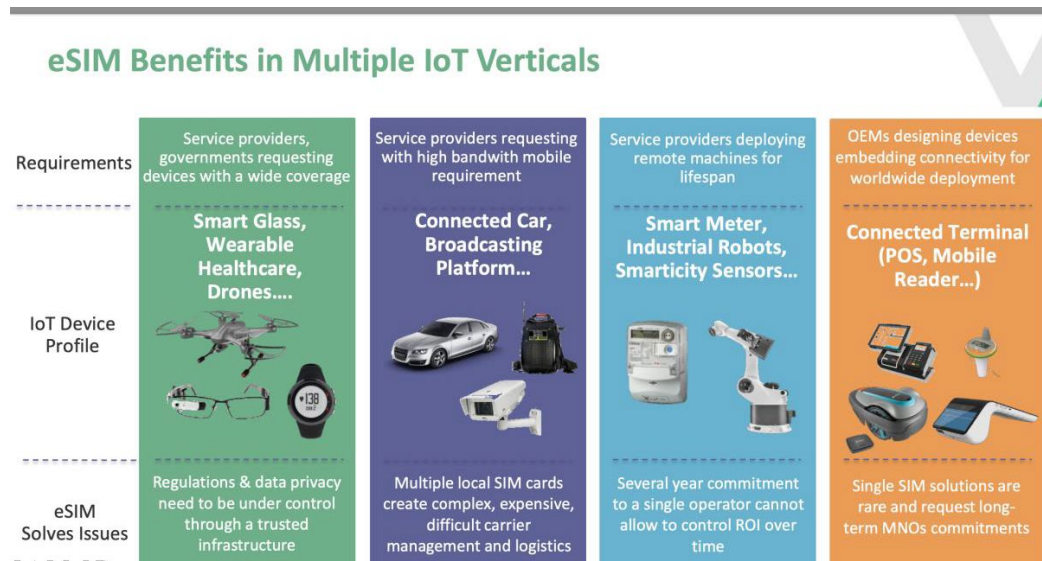


Figure 12: eSIM IoT Verticals

9.2.3. IoT Device Certificate Lifecycle Management

It is widely acknowledged that there is currently not universally standardized and publicly accessible process established for the maintenance of digital certificates for IoT devices. There is a requirement for a centralized and publicly accessible framework for Public Key Infrastructure (PKI) that can effectively manage the life cycle of digital certificates for IoT devices. The demand arises due to the significant proliferation of IoT devices across many industry sectors.

IoT device certificates are an important part of securing IoT communication. The authentication and identification of an IoT device is important to avoid impersonating legitimate devices and unauthorized to access an IoT network. Industries, such as healthcare and finance organizations are required to comply with regulations that mandate the use of device certificates. For example, the HIPAA security rule requires healthcare organizations to use device certificates to protect the privacy of patient information.

When choosing a certificate lifecycle management protocol for IoT devices, it is important to consider the following factors:

- The capabilities of the devices: Some devices may have limited processing power and memory, so it is important to choose a protocol that is efficient and lightweight.
- The security requirements of the environment: Some environments may require more sophisticated security features, such as certificate revocation and certificate chain verification.

The life cycle management of IoT device certificates encompasses several stages, including issuance, provisioning, discovery, inventory, monitoring, renewal, and revocation. The design and development of the Security Credential Management System (SCMS) and the establishment of IoT device identification will be accomplished by employing Public Key Infrastructure (PKI) technology. The composition will consist of the following elements:

- The device enrollment service includes several features, including device discovery, addition, setup, and certificate issue.
- The idea put forth includes a comprehensive management system for the lifespan of device certificates, including certificate production, revocation, and renewal functions.
- Dashboard for management and monitoring.
- Implementation of modules for specialized scenarios such as device decommissioning, device theft, faulty device replacement, and device ownership change.
- Development of Registration Authority (RA) system capable of properly verifying the identification of the owner entity.

9.2.4. IoT Identification

Identification is used for devices such as computers, servers, application gateways, RFID tags/readers, sensors, actuators, and more. They are associated with an identifier such as RFID tag identifiers, IP address, URIs (Universal Resource

Identifier), hostnames, etc. More precisely, three categories of IoT identifiers can be differentiated: (1) Object Identifiers, used for physical or virtual objects, (2) Communication Identifiers, used to identify devices when they are communicating with other devices, and (3) Application Identifiers, used for applications and services. Authentication is the process of confirming entity's identity using a login and additional information to sign in, such as passwords, PIN, smart cards, digital certificates, biometrics, etc. It is used to prevent unauthorized access to resources. Research activities can be divided into three main axes,

Cryptographic primitives and ultra-lightweight operations: Cryptographic primitives consist of hash functions (hash chain protocol, random hash-lock protocol), MACs, PRNGs, stream ciphers, block ciphers, and public keys. Ultra-lightweight operations comprise simple binary functions such as XOR, AND, OR and rotations; or NP-hard mathematical problems. Capabilities of EPC global Class-1 Generation 2; EPC global Class-1 Generation 2 capabilities intend to authenticate nodes using the 16-bit CRC and 16-bit RNG of the standard. Physical primitives utilize electronic and physical properties of RFID tags to form an authentication primitive.

The growing use of IoT in diverse application domains like automotive, healthcare and industrial control systems begs for a trust framework that is dynamic and low latency driven. Unlike conventional PKI based certificate management systems, it is essential that the specific domain requirements are adhered to before implementing a trust framework in that ecosystem. It is therefore important to develop secure certificate management systems for the IoT ecosystem, pertaining to specific application domains.

The Security Credential Management System (SCMS) and IoT device identity through digital certificates for automotive ecosystems will be designed and developed using PKI and will be powered by blockchain technology. It will comprise the following sub-objectives:

- Development of software modules for generating, validating, and disseminating Intelligent Transport System (ITS) format certificates on Intermediate Certificate Authority (CAs), for automotive applications,
- Development of enrolment & authorization process workflows in CA software, and integration with the ITS certificate CA;
- Design and implement firmware for automotive sensors which can use digital certificates for secure communication.
- Temporal and identity authentication using layering architecture would be proposed.
- Demonstration of digital certificate life cycle management and secure device communication processes on automotive sensors using PKI Trust model.
- Development of IoT device side embedded software based on Embedded Linux, for seamlessly requesting and onboarding ITS certificates, validating other device ITS certificates, and implementing process workflows for enrolment and authorization functionalities,
- Establishment of a blockchain assisted trust management framework in the PKI infrastructure to ensure tamper-proof, reliable certificate management, device lifecycle traits, and audit trails of authorization workflows,
- Demonstration of end-to-end certificate management and secure device communication processes on automotive IoT devices using SCMS backbone, authorized by Indian Root CA.

Physically unclonable function (PUF), a low-cost security feature, can be expanded to ensure hardware root security. PUF's unique characteristics, such as tamper evidence, unclonable, and on-the-fly key generation, make it a promising security primitive for IoT. With the ever-expanding domain of IoT, PUF is being utilized in a range of new applications. The PUF-enabled IoT device can provide low-cost,

unique authentication while also mitigating attacks such as tampering and cloning. Further improvements and research will be required to reach full functioning.

Identifying risk to IoT systems, assets, data, and capabilities is defined as establishing organizational understanding. The emphasis is on how organizations deal with IoT security risks, particularly in terms of resources. The process of identifying and distinguishing distinct elements inside an IoT ecosystem, such as devices, objects, or data streams, is known as "identify" for IoT. In a variety of ways, the identification process is critical for IoT adoption, including effective communication, data management, security, and personalized services.

Access management for the IoT is a critical component of the larger IoT ecosystem, since it plays a critical role in ensuring the security and integrity of interconnected devices and associated data. The process includes the control and validation of individuals who have been granted permission to access and interact with IoT devices, as well as the data generated by these devices. Effective access management protocols use authentication, authorization, and encryption procedures to defend against unauthorized access and potential security breaches. The growing number of IoT devices emphasizes the importance of strong access management in the context of IoT. This is critical for mitigating cyber threats and protecting sensitive data, establishing access management as a critical component of IoT security and operational performance.

9.2.5. IoT Protocols

IoT protocols can be divided into two categories: IoT network protocols and IoT data protocols. Data protocols mainly focus on information exchange, while network protocols provide methods of connecting IoT edge devices with other edge devices or the Internet. Each category contains several protocols that each have their own unique features and security challenges. Technologists can select from multiple communication protocols when building a network to serve their IoT ecosystem and meet the deployment security requirements. The most common protocols are CoAP, MQTT, AMQP, Wi-Fi, Zigbee, NFC, RFID, etc.

The investigation of IoT protocols is essential to the advancement of IoT networks because it improves their security, efficiency, and adaptability to the dynamic environment of networked devices and applications. This aspect is important in encouraging the long-term evolution and profitability of the IoT ecosystem across many sectors. One area of prospective research is the development and optimization of communication protocols aimed at decreasing power consumption and latency for IoT devices with limited resources. It includes investigating protocols such as LPWAN and MQTT-SN (MQ Telemetry Transport for Sensor Networks).

It will be safe to use devices with the same higher version of IoT Protocol (like Bluetooth Low Energy BLE 5.1, and not Bluetooth 4.0). If multiple devices in a network work with both lower and higher versions, the network will be effectively downgraded to the lower version of the protocol for interoperability, thus compromising the security. This is since higher versions of IoT Protocols always have better security features and mitigate various threats possible in lower versions.

The security problems raised by IoT protocols are dependent on the communication technology and standards used. The MQTT protocol may not always require strong authentication, making it vulnerable to unauthorized access. It is typical for messages to be delivered in plaintext inside the MQTT protocol, making sensitive data vulnerable to interception by unauthorized parties. The Constrained Application Protocol (CoAP) was originally designed to accommodate devices with constrained resources. As a result, it may fall short in terms of advanced security features. However, researchers can use the Datagram Transport Layer Security (DTLS) capability to improve the security of CoAP. When using inadequate or outmoded encryption techniques, Zigbee networks may be exposed to eavesdropping and unauthorized access.

LoRaWAN's lightweight design has the potential to limit the effectiveness of encryption, increasing the sensitivity of data to interception. Bluetooth device pairing procedures may contain vulnerabilities that allow attackers to intercept data or gain unauthorized access. To effectively address the security issues associated

with various IoT protocols, a comprehensive approach encompassing strong encryption, stringent authentication mechanisms, frequent security upgrades, and adherence to established best practices for ensuring IoT security is required. The protocol and its security properties should be chosen in accordance with the specific use case and the desired level of security for the IoT application.

9.2.6. IoT Access Controls

Access control aims to manage interaction and communication between users and systems. It attributes and checks authorizations to entities to execute precise operation(s). Credential management is a crucial issue in IoT context, especially regarding huge data size, leading to new implementation challenges. We classify research activities in IoT access control systems into various methods:

Context-Aware Role-Based Access Control intends to ensure context awareness and adapt security parameters to ensure the users' security according to three modular context situations: critical, emergency, and normal condition.

Cryptography-based access control (CBAC) is conceived for untrusted environments and utilizes cryptography methods to control data access. It offers benefits in distribution management, delegation support, traceability of the access, and authentication chains to extend scalability.

Users' Privacy-Preserving Access Control (UP-PAC) intends to hide user's ID and protect private information.

Trust-Based Access Control (TBAC) is a critical paradigm in the context of the IoT, which uses the concept of trust to govern device interactions and data flow inside the IoT ecosystem. The formation and ongoing measurement of trust in the methodology are dependent on a variety of parameters, including device behaviour, identity verification, authentication systems, and contextual data. The level of trust provided to IoT devices and entities determines their access permissions, reducing the possibility of unauthorized access and malicious activity. Trust-based access control improves the security and privacy of IoT systems while simultaneously

making flexible and adaptive access restrictions easier to implement. As a result, the dependability and efficiency of IoT installations in diverse application domains improve.

Investigating and developing dynamic trust models for IoT networks that adapt to changing conditions and behaviours. The research might look at how real-time data, contextual knowledge, and prior encounters affect trust levels, which could help improve access control decisions. To increase trust evaluation, the project may employ machine learning and artificial intelligence. Investigating trust-based access control solutions that preserve the privacy of IoT device owners and users. To assess and manage trust without revealing sensitive information, IoT ecosystems could use homomorphic encryption, secure multi-party computation, or zero-knowledge proofs.

The ubiquitous interaction of entities makes many operations possible, as data sharing, entertainment, and resource distribution. It leads to higher cooperation between entities and creates new sharing vectors through mobility of communicating devices, which may constitute a major object for security attackers. Consequently, it is meaningful to build up successful solutions for secure sharing.

9.2.7. Lightweight Cryptography

Introducing lightweight electronics, the reliable data security guardian, the heavyweight contender who safeguards the safety of your critical data. According to the knowledge of security professionals, the National Institute of Standards and Technology (NIST) recently pronounced a successful outcome in their endeavor aimed at creating a capable guardian for data created by small devices. The Ascon cryptographic algorithms were chosen as the winner, and NIST plans to release them as the lightweight cryptography standard.

The algorithms chosen have been specifically designed to protect the data created and conveyed by the IoT, which includes a broad array of small sensors and actuators. Furthermore, these devices are specifically designed to cater to a wide range of small technologies, such as implanted medical devices, stress monitors

embedded into highways and bridges, and keyless entry fobs used in automobiles. These devices require "lightweight cryptography" to protect their electrical resources, which are naturally limited. These algorithms are expected to cover a wide range of devices with similar resource constraints.

Ascon was created in 2014 by a consortium of cryptographers from notable institutions such as Graz University of Technology, Infineon Technologies, Lamarr Security Research, and Radboud University. Now, the Ascon family consists of seven people who have the potential to be included in the NIST lightweight cryptography standard. The multiple versions within the family give a diversified variety of functionalities, providing designers with numerous options for catering to various jobs. McKay considers authenticated encryption with associated data (AEAD) and hashing to be two critical goals in the field of lightweight cryptography. Given that Ascon comes in a variety of flavors and that only one finalist will be chosen for lightweight cryptography in authentication and key encapsulation, it would be interesting to investigate and make recommendations for all its variants based on the various verticals of IoT devices.

The AEAD cryptographic scheme is used to protect the confidentiality of a given message. However, it also allows for the addition of supplementary data, such as a message header or a device's IP address, without requiring encryption. During transmission, the algorithm ensures the authenticity and integrity of all protected data. The usage of AEAD is relevant in the context of vehicle-to-vehicle communications, as well as in reducing the danger of message forgery in the domain of radio frequency identification (RFID) tags, which are commonly used for tracking packages within warehouse environments. Hashing is the act of creating a succinct digital representation of a message that allows the recipient to determine whether any changes have been made to the message. In the context of lightweight cryptography, hashing algorithms can be used to validate the acceptability of a software update or to ensure the accuracy of the download process.

According to the NIST, the Advanced Encryption Standard (AES) as defined in Federal Information Processing Standards (FIPS) 197, in conjunction with the Galois/Counter Mode (GCM) as specified in Special Publication (SP) 800-38D, is the most effective technique for achieving authenticated encryption with associated data (AEAD). Similarly, the widely used hashing algorithm for cryptographic purposes, as described in FIPS 180-4, is Secure Hashing Algorithm (SHA-256). One of the Ascon variants provides some resistance against possible attacks launched by a high-performance quantum computer.

The importance of post-quantum encryption stems mostly from its capacity to protect long-term secret information over extended periods of time. The importance of lightweight algorithms in cryptography stems from their ability to protect fleeting secrets. The Ascon specification includes several revisions, and it is probable that not all of them will be included in the final standard. The NIST team wants to work with the Ascon designers and the larger cryptography community to obtain a consensus on the specific issues of standardization.

9.2.8. IoT Network Security Orchestration and Automation

The utilization of smart connected devices for deriving better observability of the network and providing automation of network services including security is the major trend across the globe. The trend toward virtualization of networks and network functions are growing while the hybrid and physical networks shall be in the majority for at least some more years. Out of the Cloud based and on-premises based security orchestration and automation solution deployment models, the adoption of cloud-based solutions are on the rise. The on-premises deployment model may dominate for some more years.

Autonomous Levels	L0: Manual operation & maintenance	L1: Assisted operation & maintenance	L2: Partial Autonomous Networks	L3: Conditional Autonomous Networks	L4: High Autonomous Networks	L5: Full Autonomous Networks
AN services (Zero X)	N/A	Individual AN case	Individual AN case	Select AN cases	Select AN services	Any AN services
Execution	P	P/S	S	S	S	S
Awareness	P	P	P/S	S	S	S
Analysis/ Decision	P	P	P	P/S	S	S
Intent/ Experience	P	P	P	P	P/S	S

Figure 13: IoT Network Orchestration and Automation Procedure

The complexity of networks is expected to escalate due to the simultaneous presence of on-premises and cloud service subscriptions from various providers. The specific aspects that contribute to the complexity like the volume of generated data, increased network traffic, and the rising number of network endpoints shall continue its upward growth. Managing the interconnection of diverse systems and applications in a secure manner shall be a greater challenge in this environment. To cope with increased complexity, the adoption of network orchestration and automation solutions shall become a necessity.

Big data based descriptive analytics is already adopted for a better insight of the network security and its orchestration. The application of ML/AI in the analytics shall be a major advancement in the coming years to achieve the predictive and prescriptive analytics capability. In the coming five years, predictive analytics shall be the focus and it shall also support the achievement of autonomy in the network security orchestration and automation domain. The level of autonomy in the network is defined by Forum as provided in the following table. The P depicts the manual operation (personnel) and S represents the autonomous operation (system). The network security orchestration and automation shall achieve the level of L3 in the short term (illustrated in Figure 13).

9.2.9. oneM2M

During the last two decades, the availability of affordable sensors, together with the proliferation of Internet infrastructure, enabled an interesting technology called the IoT, which has also been known as Machine-to-Machine Communication (M2M). Riding on the advancement in sensor and communication technologies, IoT/M2M continuously changes almost every aspect of present-day life. The continuous increase in the number of connected devices and the huge growth of connected devices projected in the coming years shows that M2M is the future technology that is here to stay and will proliferate in multiple sectors. In the past few years, worldwide growth in Internet usage and broadband (with declining costs) have boosted IoT/M2M.

oneM2M is the global standards initiative that covers requirements, architecture, API specifications, security solutions and interoperability for Machine-to-Machine and IoT technologies. The ITU Telecommunication Standardization Sector (ITU-T) has approved a set of security specifications for internet of things (IoT) systems. The oneM2M specifications define a common set of IoT service functions to enable secure data exchange and information interoperability across different vertical sectors, service providers, and use cases. The specifications set out in the ITU-T Y.4500.3 oneM2M security solutions document are extensive, encompassing three IoT security architecture layers: security functions, security environment abstraction, and secure environments. Security-related capabilities are an essential and complementary component in all IoT systems – oneM2M treats security as a common service function that can be applied in the same way across many applications in different verticals, It also emphasizes the use of open standards so that service providers can control all entities and services in their deployments without relying on a single company or proprietary set of technologies. The standards cover requirements, architecture, application programming interface (API) specifications, security solutions and mapping to common industry protocols such as CoAP, MQTT and HTTP.

9.2.10. MLOps and Decentralized AI/ML pipelines

With the advent of edge computing, AI processing is moving from the cloud toward the edge, allowing for fast local decisions. To make this possible it is key to explore decentralized mechanisms to orchestrate AI pipelines, i.e., the process of collecting and adapting data for model computation, the model computation and their deployment. Such pipelines will need to i) embrace MLOps able to trigger model re-computation, not only based on analyzed data, but also on the application contextual data, and to ii) integrate ways to preserve data privacy in complex and distributed IoT ecosystems (e.g., by leveraging federated machine learning architectures). Decentralized AI/ML pipelines will have a key role to increase data privacy.

Edge devices may have limited resources and capabilities to implement security measures or may be more exposed to physical attacks. AI algorithms may be vulnerable to adversarial attacks, such as data poisoning or evasion, or may generate biased or erroneous outputs. IoT security research needs to address the security challenges and risks of edge computing and AI in IoT systems, and to develop methods and tools to secure and verify the edge devices and the AI models. In recent years, major advances were made in AI software algorithms and hardware to train these models on. Many companies are working to accelerate the rate that IoT-derived data can be analyzed and turned into useful insights in data centers and at the edge. Also, with more IoT devices collecting data, there is more data for analysis and training. Once data centers have created these models, they can be implemented as an inference engine at the network edge or in IoT endpoint devices to enable new and better-performing applications. Some of these models can also learn locally, adjusting their capabilities as they gain experience with data in the field.

TinyML is one of the hottest trends in the embedded computing field right now, with 2.5 billion TinyML-enabled devices estimated to reach the market in the next decade and a projected market value exceeding \$70 billion in just five years. Dubbed Tiny Machine Learning (TinyML), it proposes to democratize the use of Machine Learning (ML) and Deep Learning (DL) on frugal Microcontroller Units

(MCUs). Traditionally, sensor data is offloaded onto models running on mobile devices or cloud servers. It is not suitable for time-critical sense-compute-actuation applications such as autonomous driving, robot control, and industrial control system. TinyML allows offline and on-board inference without requiring data offloading or cloud-based inference.

The rapid miniaturization of Machine Learning (ML) for low-powered processing has opened gateways to provide cognition at the extreme edge (E.g., sensors, and actuators). It is desirable to enable onboard ML on microcontrollers, turning them from simple data harvesters to learning-enabled inference generators, and on-device analytics for a variety of sensing modalities (vision, audio, motion, identification, etc.). The Intelligent IoT nodes at the extreme edge shall be made capable of making micro- decisions and inferences through TinyML technology. The Edge ML and the Cloud/Core ML capability shall be built as part of the network infrastructure of IoT (as shown in Figure 14). In addition to ML capability, the nodes are also equipped with eSIM/iSIM, enabling large-scale connectivity orchestration among the IoT nodes.

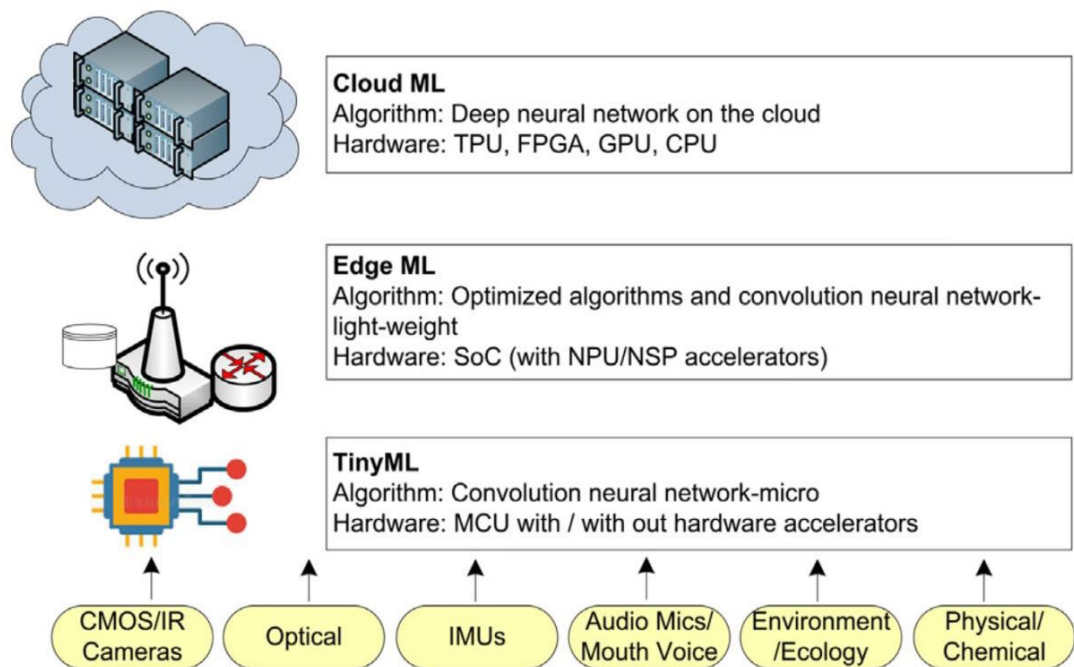


Figure 14: Embedded Machine Learning Computing Models

Embedded AI on microcontrollers is motivated by applicability, independence from network infrastructure, security and privacy, and low deployment cost. It brings the advantage that less data needs to be transmitted. Instead of sending raw data, only the results of predictions need to be sent. This way, data analytics can be performed directly on the IoT device with very low latency and low power requirements.

Privacy-centric security systems; closed-loop sensor/actuation systems, single-purpose devices that don't need connectivity, just some smarts, devices that need a super-fast response time, such as a sensor on a motor detecting a problem and stopping it before it breaks. Build devices that use less power and respond ever more quickly. With actual learning on the chip, each sensor could become personalized to the ways in which the device runs in a particular environment.

The security benefits of using local machine learning are considerable. After all, if you don't connect a device to the internet, you have a much smaller attack surface. That benefit goes hand in hand with privacy.

Deploying options of TinyML for IoT Applications

Over-the-Air (OTA) Approaches. Flashing Over-the-Air (FOTA) updates are commonplace in resource-abundant situations, there have been attempts to democratize TinyML in an OTA fashion. OTA updates provide the ability to resolve bugs and security vulnerabilities identified post-deployment or even support completely different functionality. OTA updates should be performed in a secure method to avoid an attacker injecting malicious code to the update. Use of proper authentication and confidential mechanism can be utilized for a secure OTA update.

Federated Learning model - the research in TinyML has led to breakthroughs in Reformable TinyML, i.e., TinyML solutions that can improve themselves via local or OTA updates. The edge devices update parameters of a shared model on board, send the local versions of the updated model to a server, and receive a common and robust aggregated model, without the data ever leaving the edge devices.

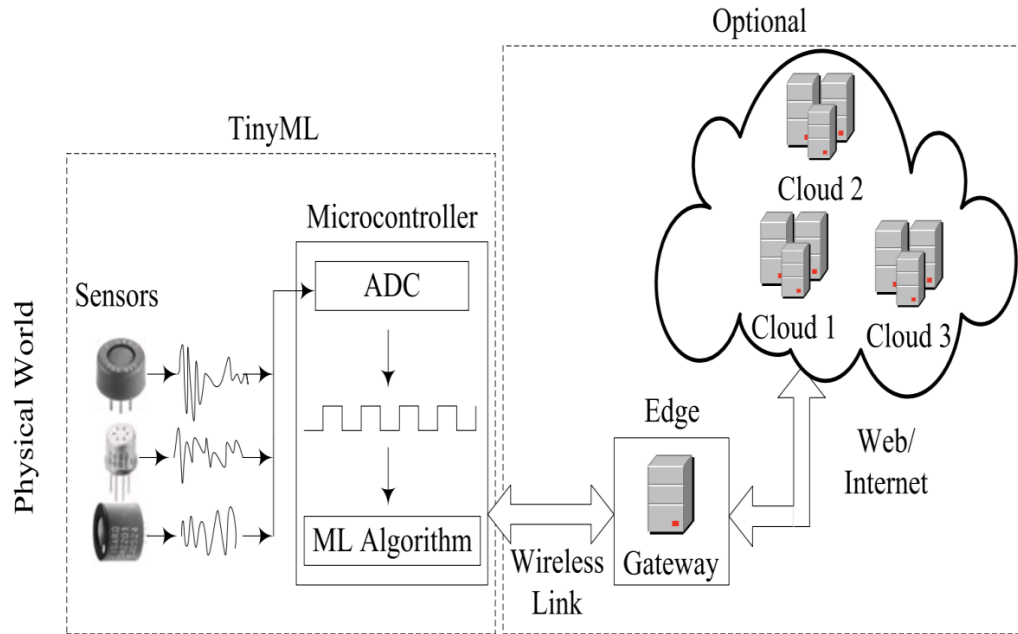


Figure 15: Working of TinyML with IoT

As illustrated in Figure 15 TinyML can be easily applied in numerous scenarios to create always-on smart applications that make predictions, process complex data, and administer solutions! Physiological applications are mainly based on behavioral metrics and include activity detection, segmentation, and forecasting.

Industry telemetry applications include sensing of different parameters from the environment, motor control, predictive maintenance, and anomaly detection. It is also noted that through modeling and analysis of signals from a wide range of sensors such as microphones, accelerometers, cameras, and gyros TinyML applications for consumers and industries are on the rise, for example anomaly detection, predictive maintenance, activity recognition, and object detections.

Security and Surveillance: Camera sensors equipped with hardware that can perform relatively fast and accurate video analytics, applied in several domains such as telehealth, security and surveillance, services, monitoring, navigational devices, etc (refer Figure 16).

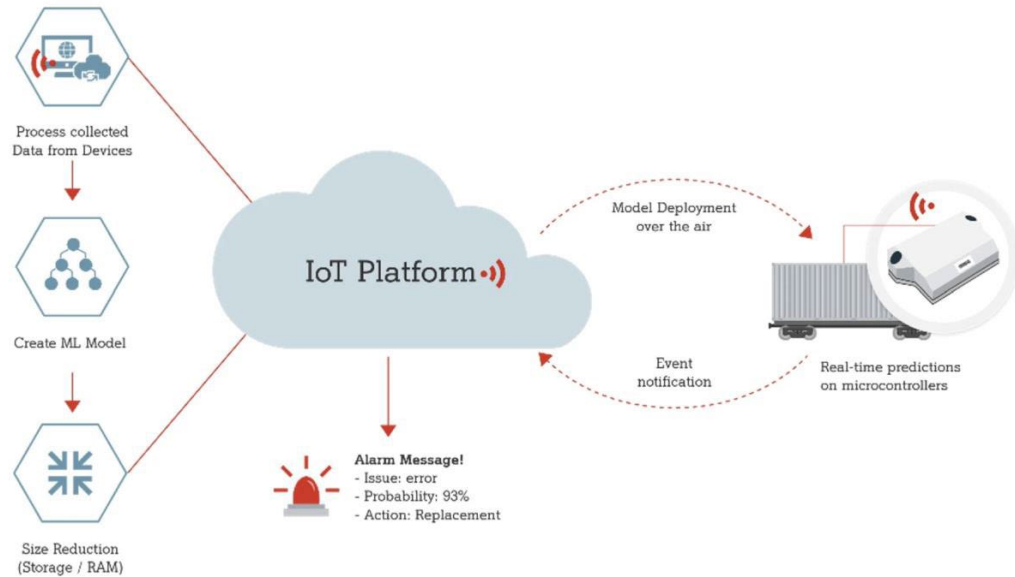


Figure 16: Real Time IoT Application scenario with Platform

Implementation of Cyber Threat Intelligence Platform on Internet of Things (IoT) using TinyML Approach

Industrial Monitoring and Control: Manufacturing and assembly line quality assurance, real-time assembly machine diagnostics, predictive maintenance, etc.

Smart and Secure Societies: Intelligent transportation systems, water distribution systems, smart energy grids, smart agriculture, disaster relief and emergency response technologies, education, etc.

Task Offloading: On/off-loading of computational tasks can be actually harnessed during edge enabled machine learning scenarios. Such loading strategies should be an add-on to existing dynamic configuration of edge-aware specifics. Doing so, TinyML can empower the transfer of resource-intensive jobs from the resource frugal edge devices.

9.2.11. Blockchain assisted IoT Security

Blockchain provides a distributed and shared ledger that is maintained as chained blocks, each containing a set of transactions. The chaining is achieved using cryptographic hash that is derived from the previous block, which makes them

immutable. Each entity in Blockchain is authenticated using proven public key cryptography and the transactions are signed and verified using digital signatures. These features of Blockchain make it suitable for monitoring and tracking the lifecycle of IoT devices, often deployed in massive volumes for specific application domain use cases. Agents residing on the device would maintain a periodic update of the device functions, bring in traceability and device lifecycle state, even though the device is deployed in target application domains. Some interesting use cases feasible through blockchain integration are:

- Device enrollment and ownership management including commissioning and decommissioning of the device in the IoT network.
- Credential management for IoT to ensure authorized access with strong authentication mechanisms.
- Periodic & On-demand device scan for recording security artifacts
- Privacy management of Sensor data along with IPFS enabled storage.
- Audit Trail of IoT device functions like configurations, firmware updates, device authentication, device connections

9.2.12. Theft and Tampering of IoT devices

Security and fraud domains are beginning to interconnect and largely driven by the switch to IP networks, which makes Internet Service Providers (ISP) more vulnerable. Network Security vulnerabilities initially used by hackers to cause website outages or create other havoc are now being exploited to commit telecom fraud. The theft of a smart device (IoT consumer/Industry 4.0), smartphone or smartwatch, or tablet entails not only a financial burden: Even more serious is the loss of valuable data, be it contact and account information, image files, or passwords. The only way to protect the data is as soon as possible after the theft is to lock the device. For this purpose, network operators place missing registered mobile devices on an internal, locally stored blacklist based on the International Mobile Equipment Identity (IMEI). Once this is done, the thief can no longer dial

into the network using the stolen device. The solution prevented thieves from connecting to the same network with the stolen device but didn't prevent them from connecting to other networks. The challenge was creating a trusted Global unified IMEI blacklist that network operators, smart device (IoT/Mobile) manufacturers, and end users anywhere could use to list and identify blacklisted devices. It would be great to suggest some FIR/complain mechanisms where someone complain if he/she received any devices without IMEI number or cloned IMEI number and how to verify IMEI number authentication without revealing the original IMEI number.

Using blockchain to secure IoT ecosystem deployments would help tackle the physical theft of smart devices. A smart device that is either reported to the IoT blockchain network as being stolen or identified by the network as behaving according to a set of criteria that correlates as having been stolen could immediately be quarantined by the network and have its important data forwarded to the police and owners, etc.

Information such as the smart devices' current location and even secret pictures taken by the operator through surveillance cameras could be automatically sent to the nearest police officers without needing 3rd party intervention. The devices' unique manufacturing number could also be automatically shared with organizations such as the OS provider and other application platforms, enabling them to blacklist the device. It would prevent the current problem of thieves simply performing a factory reset and using the device for themselves. The system will combat device theft, fraud, harassment, data loss, and identity theft-related crimes through blockchain ledger. Secondly, digital assets management, data protection and remote provisioning system is deployed in devices with eSIM technologies. Incorporating Blockchain with eSIM in the telecom ecosystem will improve the security of critical assets and reduce the chances of device theft, identity/device spoofing/swapping frauds, and security/privacy breaches of the users and devices.

Additionally, further services or products could be built. Some examples would be:
a) access for public authorities like the police to verify device ownership and status

of a device, b) products for the insurance industry where verifiable information about the theft is relevant, c) services to provide ownership/status information on devices being traded on the second-hand market.

9.2.13. New Chip design and Standards

In addition to the system disaggregation, traditional semiconductor device design is undergoing its own disaggregation with the introduction of chiplets. Chiplets separate many of the traditional CPU functions into separate smaller chips that are connected to each other with high-speed interconnects on a small package. In 2022, a new standard, called Universal Chiplet Interconnect Express (UCIe), was introduced that will enable specialized chips from many manufacturers to be combined together in a compact package. It enables the creation of more specialized semiconductor chiplet packages for special applications and creates the need for a new type of foundry for assembling chiplets into a UCIe package. UCIe will enable more efficient semiconductor devices for data centers, the network edge and IoT endpoint devices. Disaggregation of traditional data center servers and composing virtual computing systems enable more efficient data processing, as well as lower power consumption. Much of the data processed in data centers is from IoT applications, and as IoT grows, processing will grow. Non-volatile memory express, Compute Express Link and the changes.

9.2.14. Artificial Intelligence of Things (AIoT)

AIoT refers to the integration and fusion of two independent technology fields, namely Artificial Intelligence (AI) and the Internet of Things (IoT). The method comprises incorporating artificial intelligence capabilities into IoT devices and networks to increase their usefulness and intelligence. The incorporation of AIoT enables IoT devices to handle data processing, analysis, and decision-making activities more effectively. As a result, integration improves the development of real-time insights and increases device autonomy. AIoT refers to the use of machine learning methods, computer vision, natural language processing, and other artificial intelligence techniques. It will allow IoT devices to constantly adjust, acquire

knowledge, and gradually improve their operational capabilities. The combination of AI with the IoT not only improves device intelligence but also opens up new potential in domains as diverse as predictive maintenance, healthcare, smart cities, and industrial automation. This integration makes it possible to do more complex data-driven decision-making and automation procedures.

Furthermore, the incorporation of AIoT plays a critical role in efficiently addressing the data management and security challenges inherent in the IoT. AI algorithms can aid in the discovery of anomalies, the detection of security concerns, and the effective handling of large amounts of data generated by IoT devices. By introducing AI into IoT ecosystems, companies may successfully exploit the full capabilities of their networked devices while simultaneously ensuring data privacy and security in an increasingly complex and data-abundant environment.

9.2.15. Zero-Trust Architecture

Zero Trust Architecture (ZTA) implementation is a critical method for improving the security of IoT systems. It entails strict implementation of access control mechanisms as well as continual monitoring, with no assumptions about the trustworthiness of devices or people within the network. Within the context of the IoT, ZTA requires that each device, including sensors, actuators, and gateways, go through stringent authentication and authorization procedures before being granted access to network or data resources. This methodology ensures that no device is inherently deemed trustworthy in a system of interconnected components, and authorization is only granted based on the necessity of information and activities. As a result, successfully reduces possible points of vulnerability and impedes attack transmission across the network.

Furthermore, the IoT Zero Trust Architecture places a strong emphasis on the ongoing process of continuous monitoring and risk assessment. Devices are evaluated on a constant basis to determine their performance and compliance with security laws. Any deviation from expected behaviour or indicators of compromise can induce rapid and decisive measures, such as device isolation or revocation of

access privileges. The presence of a real-time capability for detecting and responding to threats is critical in ensuring the security and integrity of an IoT network, especially when managing many interconnected devices that may contain vulnerable or compromised endpoints. Implementing ZTA in the IoT can dramatically improve an organization's security posture, preserve sensitive data, and manage the growing risks and vulnerabilities associated with IoT deployments.

It is regarded vital to improve access control and identity management inside an IoT environment by utilizing ZTA concepts. It may include a comprehensive set of access control policies that strictly adhere to the essential ideas of Zero Trust. Please include information about the specific devices or users who can access the system, as well as the requirements or criteria that should be completed to acquire access. Furthermore, durable device authentication mechanisms such as mutual Transport Layer Security (TLS), digital certificates, or biometric authentication may be developed to establish a secure connection exclusively for trusted devices within the network.

9.2.16. AI Enabled Privacy and Data Protection

Another challenge in IoT security research is the privacy and data protection of the data generated, collected, and processed by IoT devices and applications. IoT data can contain sensitive and personal information, such as health records, location, preferences, and behavior. Data can be exposed to unauthorized access, modification, or leakage due to weak encryption, insecure storage, or malicious attacks. IoT security research needs to address the privacy and data protection issues of IoT data, and to ensure that the data is handled in accordance with the legal and ethical requirements and the user's consent and preferences. IoT security research also needs to consider the trade-offs between privacy and functionality, and to provide users with transparency and control over their data. While several of the challenges discussed above have a primary focus on technology, there is an important challenge unrelated to technology that needs proper attention for the development and adoption of Next Generation Internet of Things solutions.

The wider the adoption of IoT, the wider the ‘intrusion’ of devices and ‘intelligent’ services will be in our everyday life. What is an acceptable level from a citizen’s perspective? What are the ethical implications that Next Generation Internet of Things solutions need to face? How is it possible to make what happens behind the curtains more transparent to ensure that intelligent solutions can be trusted? How can such solutions ensure compliance with GDPR, as well as with future regulations? How can citizens be truly aware of the decisions they are making with respect to data processing? How can we ensure an inclusive approach to IoT and counteract possible inequalities that might emerge with the wide adoption of IoT? And as connectivity intensifies, citizens will increasingly request spaces of disconnection. How can we facilitate these requests? This challenge is clearly demanding for a multidisciplinary approach embracing legal, sociological, and ethical research in relation to the adoption of IoT and connected technologies, such as Artificial Intelligence. Innovations in privacy-preserving techniques, like homomorphic encryption and differential privacy, enable data analysis while protecting user privacy. These innovations will facilitate the secure use of personal and sensitive data in IoT applications.

Data privacy should be considered throughout different phases of data usage, including collection, transmission, and storage. During data collection and transmission, we need to focus on networking issues and technologies such as RFID, WSN, and mobile connectivity. In the storage and processing phase at collection nodes, guaranteeing data confidentiality and integrity and implementing adequate security techniques must occur. Effective solutions include anonymization, block ciphers, stream ciphers, hash functions, lightweight pseudo-random number generator functions, and lightweight public key primitives. These techniques are generally combined to provide the required level of privacy depending on the sensitivity of data, network settings, and application and user requirements.

The major violation/update has been happening during the change of the ownership of the service providers in any service based on the data collected from IoT devices.

There should be some basic checklist during the new update of the privacy policy so that a customer can be able to know the changes done in the new update.

It emphasizes the way people can access personal information. It is important to highlight the need for efficient policies and mechanisms to manage different data types and fit various situations in IoT contexts. It may include blocking approaches, lightweight protocols data sharing, and accessing techniques.

Devices are considered one of the more exploitable entry doors for cyber-attacks. Thus, it is essential to advance research related to their security, including solutions for on-chip encryption, hardware-software integrated security functions, and tamper-proof technologies. While privacy by design in data is largely explored, additional research on device privacy is required to increase trust toward IoT.

Recently there have been more and more breaches of sensitive data, and attacks on critical infrastructures. Increased security of IoT infrastructures is central to the safety and security of several applications and their users. On the security side, it is fundamental that research strengthens methods for development of secure architectures including new methods and tools for formal verification of specifications, designs and implementations to detect possible security threats. Artificial Intelligence may play a key role into supporting such methodologies and in the development of cyber threat solutions (model-level proofs, source code analysis, binary analysis, hardware analysis, etc). As regards privacy, many research aspects are yet to be explored, including ways to automate Digital Personal Data Protection Act (2023) compliance tests, solutions to provide privacy-preserving data processing and machine learning (for which distributed ledgers may provide interesting solutions), mechanism to generate dynamically data access control policy based on different context parameters while preserving data privacy.

9.2.17. Self-Adapting Intrusion Detection System

As the massive IoT environment is dynamic, adapting to changing attacks and detecting new attacks is needed. Applying Generative Adversarial Network (GAN) in the context of IoT security endows a defense mechanism with a powerful means

to discover unknown attacks as it learns various attack patterns to produce samples like zero-day attacks. Also, reinforcement-learning-based IDS has a strong potential to realize self-adaptation in dynamic environments.

9.2.18. IoT and IoTA Tangle Distributed Ledger

In traditional blockchain models, transactions are bundled in each block after getting verified by the miners. So, as the number of transactions increases, the work for miners also increases. In more and more IoT scenarios, distributed ledgers are key enablers for secured and trusted data exchange and distributed processing. However, their application in real time scenarios is still not possible given that current distributed ledger solutions introduce additional latency in the data management and have high computing costs. Proper solutions need to be explored to allow adoption of distributed ledgers at the scale and latency required by real time IoT scenarios. There is a need for Highly scalable and low latency ledgers for IoT.

IOTA is based on a new distributed ledger, called Tangle, which overcomes the inefficiencies of the current blockchain design, introducing a new method of consensus in a decentralized peer-to-peer solution. In IOTA, instead of a global blockchain, we have directed acyclic graph, called Tangle. The Tangle graph is the ledger for storing the history of all transactions.

As opposed to that, in a Tangle architecture each transaction will form a new block and will be verified by itself. To carry out the verification, it needs two randomly chosen transactions in the same network. IOTA's is decentralized and is indefinitely scalable with zero cause, allowing us to build a self-sustainable economy on-demand. Perfectly fitting the next generation business models.

IOTA positions itself as being an ideal distributed ledger for IoT due to its feeless nature and scalable distributed structure. Obviously when architecting any smart system, the developer needs to compromise between various factors such as price, speed, reliability, security and so on. An IOTA-based IoT system will automatically include secure logging of all events and therefore could be used for charging customers on an event-by-event basis. A hybrid system could also be envisaged

where some frequent but low risk transactions could be made using a standard MQTT transport (e.g. continuous tracking of the location an ARV), whereas infrequent but chargeable events could be made using a secure system like IOTA (e.g. credit card payment for an entire trip).

Recently, the IOTA Foundation has signed a collaboration agreement with the International Transportation Innovation Centre (ITIC) to create test systems (testbed) aimed at the world of “intelligent mobility,” also known as smart mobility. ITIC's goal is to create a testbed network capable of incubating and validating sustainable mobility services based on artificial intelligence (AI), using physical (real) test methods or based on virtual and augmented reality.

IOTA's Tangle architecture could be used as an infrastructure for exchanging messages and data acquired by the sensors. These type of sensors could also be placed in private homes in the future, in which case the owners of the buildings would become suppliers of service to the structures that deal with environmental monitoring.

While blockchain certainly has the components necessary to support micropayments in an IoT environment, it does have its disadvantages. Most notably, questionable security, an inability to personalize, and an overall lack of convenience when it comes to usage. IOTA was designed to provide these qualities and more. Compared to other major electronic payment methods, its three advantages are the fact that it is modular, decentralized, and not subject to taxation. IOTA is essentially created to ensure that transactions can occur without being subject to any commission.

9.2.19. High Performance Computing (AI capable) devices for the edge

Nowadays cloud offer includes different specialized capacities, including GPUs and other AI and ML specific hardware design allowing to speed up training and inference in the cloud. Clearly, while there is space for research and improvements in the AI-enabled computation in the cloud, the major research challenge of today

reside elsewhere. To improve performance of IoT- related data processing and decision making, developing devices with novel processing capacities is key. Advancements in AI specialized processors are required. Good progress has been made toward processing units capable of performing machine learning and deep learning tasks at the edge. Current research shows that AI specialized processors can achieve 10 times the performance of GPUs and FPGAs. Still, capacity may not be enough with the increasing volume of data that will be generated and new research developments such as neuromorphic computing should be investigated. While achieving this goal, research should also ensure that energy usage is kept under control.

9.2.20. 5G and IoT

The 5G, 5G-Advanced mobile network shall become the main mode of connectivity for IoT devices soon. The control and data plane are separated in the 5G network where user data is handled by data plane. The control plane security is well defined as part of 3GPP standards while most of the data plane security mechanisms are made optional in the standard. The orchestration of end-to-end network security in the 5G and beyond network shall be a major challenge and technology development shall focus on these aspects.

While LPWAN solutions have been largely tested and offer a low-cost solution for large IoT deployments, they suffer several drawbacks in terms of supporting real-time and high- bandwidth scenarios. Despite the fact that NB-IoT and LTE-M appear to be initial solutions to the open challenge, they fail in some respects. On the one hand, NB-IoT, designed with increased reach and lower cost and power consumption, offers limited bandwidth and latency around 1 sec. On the other hand, LTE-M, while providing higher bandwidth, fails on the low- cost constraint. It implies that the road to provide large-scale deployment, able to support real-time scenarios with bidirectional communication at a low cost, is still a challenge.

5G and its evolution should go further to address the low cost, massive device deployment. Such technologies need as well to be sustainable by limiting the usage

of resources and the impact on the environment, to avoid the large-scale deployment of devices becoming unsustainable from an environmental point of view. The forecasted increasing number of devices we will witness in the future will make the challenge more pressing, it relates to optimizing IoT integration into the global Internet, with a focus on IPv6, as well as in cellular networks, such as 5G (and other future networks), but it entails research as well in relation to energy and sustainability of IoT devices.

5G offers to corporates important benefits in terms of data speed, latency, reliability, efficiency, capacity and security. 5G is, therefore, expected to support a wide array of new solutions. Some of the benefits of IoT could be realized within an existing telecommunications infrastructure, but previous wireless technology generations do not have the capability to integrate with autonomous robots or advanced technologies. In contrast, when IoT is combined with 5G networks in a transformation strategy, the goals of Industry 4.0 come within reach.

While private networks have always existed, they'll start to mature in 2024. Enabling secure and seamless roaming between private and public networks is vital since switching between the two is not intrinsically safe. In addition, new technologies are giving rise to solutions. Enterprise Network Operators (ENOs) play an important role here.

Traditionally, enterprises have worked with either MNOs or MVNOs to power their mobile networks. However, neither of these has been ideal solution to meet enterprise needs properly, given the drawbacks of siloed networks with complex roaming agreements, which lack centralized control and increase IoT security threats. As a result, enterprises need tailored network services now more than ever, and in 2024, ENOs will meet this need.

ENOs combine the best features of both MNOs and MVNOs to put owners of the network into the hands of the enterprise and provide completely tailored solutions, including more secure IoT connectivity. The coming year will see more of these kinds of technologies taking root within businesses as enterprises seek to regain

control over their data security and fortify their digital assets. In fact, 92% of enterprises say they plan to use private networks by 2025, so expect 2024 to be the head start towards that future.

5G/6G networks will rely heavily on network slicing to cater to various IoT use cases. Research is focused on securing these slices individually to prevent interference and ensure the privacy and security of data within each slice.

9.2.21. Enhancement in the Automotive Security

The security ecosystem of Automotive IoT is comprises of various stakeholders - Automakers (Original Equipment Manufacturer - OEMs), Tier 1 Suppliers, Telematics Service Providers, IoT Platform Providers, Software Developers, Regulatory Bodies and Governments, Insurance Companies, Fleet Management Companies, Infrastructure Providers, Cybersecurity Firms, Aftermarket IoT Suppliers, Consumers, Dealerships and Service Centers, Environmental Agencies, Data Analytics and Machine Learning Companies, Smart Cities and Urban Planners. Efforts form Multiple Parties are required for securing the entire digital lifecycle of modern vehicles.

Since OEMs source a large share of their vehicle components from suppliers and semiconductor manufacturers, their upstream value chain partners will also be required to follow and implement state-of-the-art practices to mitigate cybersecurity risks and produce vehicles that are secure by design.

These partners must provide evidence of adhering to the regulations and security standards, which is the responsibility of the OEM.

The value chain is affected across four areas:

Cyber-risk management through Vehicle Security Operations Centres: It is the responsibility of automotive industry participants to implement end-to-end cyber-risk management, identify pertinent cyber risks in their vehicle models (and adjacent ecosystem components that may affect vehicle safety or security), and implement countermeasures. This involves responding to threats as they evolve. Vehicle

Security Operations Centres are entities that oversee irregularities in vehicles that are connected. OEMs have the option of constructing and operating SOC's internally or procuring them from external providers, such as a managed service. Specialized personnel are required to operate vehicle SOC's and respond to auto security incidents. The markets for cybersecurity processes and cybersecurity solutions present numerous avenues for establishing new enterprises. Opportunities will present themselves for testing, inspection, and certification providers in every subcategory within the domain of process conformance.

Security by design: It is imperative for OEMs to design, manufacture, and test vehicles for security vulnerabilities and adequately mitigate any cyber risks. This entails implementing cutting-edge practices in hardware and software engineering and ensuring that all vehicle types are secure from the outset. Even though OEMs bear the ultimate responsibility for cybersecurity, every participant in the value chain must contribute.

Detection and response through AI: The manufacturers must be proficient to identify technological flaws and security problems (like cyberattacks) in their automobiles as well as nearby ecosystem elements (such the back end or outside services) that might compromise the security or safety of their vehicles is a need. The utilization of AI to identify automotive attacks is an essential element in safeguarding the cybersecurity of autonomous and connected vehicles. By analyzing massive quantities of data in real time from a variety of vehicle sensors, networks, and communication channels, AI can be utilized to detect and respond to potential security threats. Key methods and techniques for automotive attack detection utilizing AI include the following:

Safe and secure updates: To address security vulnerabilities, automotive players need to be able to react to any identified security incident and release software upgrades. To accomplish this, they must methodically identify the cars that need to be updated, make sure that software upgrades are compatible with the configuration

of the vehicles, and guarantee that they won't damage approved safety-relevant systems.

9.3.Mid Term (Next 10 years)

9.3.1. Trusted Components and Reusable Certifications

The imperative to prevent threats necessitates the expansion of the repertoire of trusted components available for utilization by device manufacturers. Certification plays a vital role in demonstrating the security credentials of a component to device manufacturers, enabling them to make well-informed purchase decisions based on the knowledge. The implementation of independent certification offers advantages to the entire ecosystem by offering an impartial evaluation of a product's integrity using a standardized benchmark. It facilitates a quicker product launch and enhances customer trust. The Software Bill of Materials (SBOM) is a detailed record that lists all software components and their associated dependencies that are used in an application or system. A Software Bill of Materials (SBOM) plays an important role in enhancing security and establishing trustworthiness in the world of IoT and trustworthy components.

9.3.2. PQC Enabled IoT System

Post-Quantum Cryptography (PQC) is a burgeoning discipline within the realm of cryptography, which is dedicated to the advancement of encryption algorithms and methodologies that exhibit resilience against potential threats posed by quantum computers. The utilization of quantum computers possesses the capability to compromise numerous encryption techniques presently employed, so raising substantial apprehensions regarding the security of IoT systems and other digital communication platforms.

Developing and adopting post-quantum cryptographic algorithms will be crucial to safeguard IoT systems against future quantum threats. Select the PQC algorithms suitable for IoT devices. It is critical that these algorithms have robust security protections in place to survive potential quantum attacks, as well as adequate

efficiency to work efficiently on IoT devices with limited resources. NTRUEncrypt, lattice-based cryptography, and hash-based encryption are all examples of PQC algorithms. It is essential for ensuring that PQC is seamlessly integrated into the pre-existing security procedures of the IoT system. This may include protocols for establishing secure communication channels between devices and cloud services.

Adoption of quantum-safe communication protocols, such as Quantum-Safe Transport Layer Security (QS-TLS) and Internet Key Exchange (IKE), to secure data in transit. Global standards and guidelines for quantum safe IoT security will begin to take shape, helping IoT manufacturers and organizations implement best practices.

9.3.3. Low-power Quantum Random Number Generator (QRNG)

Quantum random number generators (QRNGs) get their random numbers from quantum processes that possess inherent indeterminism. The challenge of predicting numbers generated by QRNGs is not solely attributed to their complexity, but rather rooted in the fundamental impossibility of predicting random numbers. It may be argued that even nature itself lacks knowledge of these random numbers prior to their generation. When a photon interacts with a symmetrical beam splitter, it enters a state of quantum mechanical superposition, wherein it simultaneously exists in the states of "having been transmitted" and "having been reflected" after passing through the beam splitter. Subsequently, one of the detectors randomly detects the phenomenon and generates a stochastic binary digit. Quantum Random Number Generators (QRNGs) possess several notable advantages, including the ability to harness the inherent randomness found in nature and their straightforward operational principles. Therefore, it is possible to construct a practical physical model of a Quantum Random Number Generator (QRNG) that can serve as a foundation for certifying the generated random numbers. A QRNG has a strong attack resistance and usually the post-processing (random-ness extraction) is conceptually easy. Nevertheless, the task of developing a compact and cost-effective

quantum random number generator (QRNG) or one with exceptional speed poses significant difficulties.

9.3.4. AI Enabled Botnet Detection and DNS Ecosystem

It is projected that the IoT would facilitate a period of heightened connection, as around 100 billion devices are anticipated to be interconnected with the Internet by 2025. The primary objective of the Internet of Things (IoT) is to provide connectivity between devices that were previously unconnected, thereby enabling the development of smart home gadgets capable of autonomously collecting, storing, and exchanging data without the need for external connection. The bulk of IoT devices are designed for customers that prioritize cost-effectiveness and ease of use, often prioritizing deployment over security measures.

A botnet refers to a group of many bots that are employed for the purpose of launching attacks on a specific network. These bots are under the direction of a single entity, known as the botmaster, who manages them through the utilization of a command-and-control protocol. Bots refer to compromised computer systems that are utilized for executing harmful activities under the remote command of a botmaster, while exhibiting no discernible indications of unauthorized access. The magnitude of a botnet can vary, spanning from a modest assemblage including several hundred bots to a substantial network encompassing over 70,000 hosts. Hackers possess the ability to disseminate botnet software, engage in clandestine operations that evade detection, and sustain their productivity over extended periods of time. The subsequent obstacles should be addressed to effectively detect and mitigate botnets in IoT environments:

- The deployment of resource-intensive detection algorithms on IoT devices is challenging due to their constraints in processing power, memory, and bandwidth.

- The IoT encompasses a diverse array of hardware, software, and communication protocols. The diverse nature of these devices is a significant obstacle in the development of universally applicable detection systems.
- IoT devices frequently exhibit vulnerabilities that can be exploited because of having old firmware and a dearth of security updates. The task of identifying and addressing zero-day vulnerabilities presents significant difficulties.
- Traditional intrusion detection systems often utilize rule-based or signature-based approaches, which may be inadequate in identifying minor irregularities within Internet IoT network traffic.
- Botnet operators consistently modify their strategies in order to avoid being detected. In order to maintain concealment, individuals may employ various strategies such as command and control server hopping, domain generation methods, and fast-flux DNS.
- The presence of IoT devices is frequently distributed across many networks and physical places, leading to the occurrence of network fragmentation. It presents a significant difficulty in efficiently monitoring and safeguarding these devices.
- Numerous IoT devices employ secure communication protocols that entail encrypted traffic, hence rendering the interception and analysis of network data for indications of botnet activity challenging.
- The monitoring and detection of IoT ecosystems pose a huge problem because to the vast number of devices involved, which can reach millions in scale.
- IoT devices frequently gather data of a sensitive nature. The implementation of detection techniques necessitates careful consideration of privacy concerns and adherence to regulatory frameworks, such as the General Data Protection Regulation (GDPR).

9.3.5. 5G and 6G Transition Security

The Sixth Generation (6G) of mobile networks offers the promise of a global interconnected system, serving a large set of applications across multiple fields such as satellite, air, ground, and underwater networks. It will evolve towards a unified network compute fabric that facilitates convergence across ecosystems, fostering design and innovation of new Internet of Things (IoT) applications and services, further leading to an exponential growth of IoT use cases in the post-6G era. This profound evolution will also contribute to further evolving the threat landscape, adding new threat actors, and leading to a new set of cyber security challenges. 6G innovation can occur at multiple layers, including network architecture, communication protocols, network intelligence, and so on. communication services that will be provided by the 6G architecture:

In the IoT domain, new service classes for 6G are intended to improve on service classes of the 5G core, such as enhanced Mobile Broadband (eMBB), massive Ultra-Reliable Low Latency Communications (mURLLC), massive Machine Type Communications (mMTC), extremely high Reliability and Low Latency with Security (eRLLCS), eMBB-Plus and Secure ultra-reliable low- latency communications (SURLLC) and 6G-Lite (Cooperative Intelligent Transportation Systems, C-ITS). 6G will be a significant enabler for future IoT networks and applications, as it will provide full- dimensional wireless coverage and integrate all functionality, including sensing, transmission, computation, cognition, and fully automated control. In fact, compared to the 5G mobile network, the next generation 6G mobile network is expected to give massive coverage and enhanced adaptability to support IoT connectivity and service delivery.

The 6G network will integrate various capabilities such as communication, sensing, computing, and intelligence, making it necessary to redefine the network architecture. The novel network architecture should be capable of being flexibly adapted for tasks such as collaborative sensing and distributed learning to proliferate AI applications on a large scale, where trustworthiness should be guaranteed as a

native feature. The concept of "trustworthiness" here covers topics including security, privacy, resilience, safety, and reliability.

A critical study area is ensuring a secure transition from 5G to 6G. It includes identifying potential vulnerabilities during migration and designing security mechanisms to prevent or mitigate risks.

9.3.6. Self-sufficient Intelligent Network (AI)

It is evident that AI could not be applied to the previous versions including 4G and lower generation. However, in the 5G networks a partial or limited applicability of AI will be observed. Most prominently, the 6G networks would provide the full automation through AI which will offer full potential of the radio signals, also allowing the cognitive radio to intelligent radio-based transformations.

9.3.7. Satellite Connectivity

Satellite connectivity is expected to be an alternative to grounded and UAV-supported communication technologies for providing the purpose of the system for electronic objects on the ground and may thus be used in IoT scenarios. Some companies are developing dedicated satellites for IoT networks, encouraged by the major benefits of satellite-assisted IoT communications.

9.3.8. RISC-V based Secure SoC for IoT

The development of a secure System-on-Chip (SoC) for IoT applications, utilizing the Reduced Instruction Set Computer -V (RISC-V) architecture, is being pursued. The current necessity lies in the development of a secure System-on-Chip (SoC) for IoT EDGE devices and gateways. The implementation of the approach will effectively mitigate the risk posed by hardware Trojans in their entirety, making it imperative to include it within the scope of the Digital India RISC-V (DIR-V) programme.

9.3.9. UAV assisted Wireless Communication

UAV-assisted communications are expected applications for 6G-enabled IoT networks. UAVs can prevent biogeographic wireless communication limitations such as ships at sea, sensors in remote locations, and areas outside of terrestrial connectivity zones.

9.3.10. Digital Twin

The digital twin is a novel industrial control and automation systems concept which is identified as a key 6G application. A digital twin is defined as a digital or virtual copy of a physical object, an asset, or a product. Digital twin interconnects virtual and physical worlds by collecting real-time data by using IoT devices that are connected to the physical system. These collected data will be stored locally on decentralized or centralized cloud servers. Then, the collected data will be analyzed and evaluated in the virtual copy of the assets. After obtaining the simulation results, the parameters are applied to the real systems. Integrating data in real and virtual representations will help optimize the performance of the physical assets. Digital twin can be used in other use cases such as Industry 5.0, Automation, healthcare, utility management and contractions.

The biggest security challenge in the digital twin system is that an attacker can intercept, modify, and replay all communication messages between the physical and digital domains. With the popularity of digital twin systems in future, 6G should support highly scalable secure communication channels. Another issue in digital twin systems is that the attacker can modify or alter the IoT data and make privacy attacks. When 6G is used to enable digital twin system, IoT data integrity and privacy protection mechanisms should be utilized. For instance, blockchain can be used as a candidate technology to enable such features in 6G networks.

9.3.11. Collective Intelligence: AI-Enhanced Automotive Security and Threat Anticipation

An advancement in security is achieved with an AI-enabled automotive security system that not only provides robust intrusion detection and threat prevention, but also has the capability to learn and adapt. By analyzing user and intruder patterns across multiple vehicles, this AI system is capable of effectively anticipating and countering potential attacks.

By utilizing machine learning algorithms, the AI is capable of perpetually acquiring knowledge from patterns of user behaviour as well as any unauthorized activities that occur across a broad range of vehicles. By acquiring an exhaustive comprehension of the parameters that define typical conduct in the automotive ecosystem, it becomes capable of differentiating authorized users from potential hazards.

Through the consolidation of data from multiple vehicles, the system can detect and forecasting assault patterns or suspicious activities that may be imperceptible in the context of a solitary, isolated vehicle. It can identify prevalent intruder strategies and adjust its defense mechanisms accordingly.

When faced with an attack, the system can swiftly detect and respond to emerging threats by utilizing this collective knowledge. By leveraging historical data and pattern recognition, it can detect potential attacks, establishing itself as an intelligent and proactive safeguard against cybersecurity threats.

The adoption of a collaborative and knowledge-sharing approach among various vehicles enhances the security and safety of the automotive ecosystem, while AI consistently improves its capabilities in detecting and preventing threats. This showcases the capabilities of artificial intelligence in not only addressing established threats but also foreseeing and minimizing forthcoming hazards.

9.3.12. Automotive Supply Chain attacks – Risk mitigation strategies

Supply chain vulnerabilities in the automotive sector pose significant threats to the safety, security, and performance of vehicles. These vulnerabilities include issues like counterfeit components, third-party software, data protection, insider threats, geopolitical and environmental factors, intellectual property theft, and adherence to compliance standards. To mitigate these risks, automotive companies must implement rigorous strategies and ensure alignment with industry-established standards.

To combat counterfeit components, stringent supplier qualification processes, traceability technologies, thorough security assessments, and penetration testing are essential. Data privacy and security are crucial, with measures like encryption, strict access controls, and adherence to data protection regulations. Insider threats require background checks, access controls, and fostering a culture of security awareness. Geopolitical and environmental factors, such as political instability and natural disasters, require diversifying suppliers and locations and maintaining contingency plans. Intellectual property theft requires protective measures like patents and trade secrets. Compliance with industry-specific standards and regulations is crucial in reducing risks associated with non-compliance.

To effectively secure the automotive supply chain, a comprehensive approach that includes best practices in security, robust supplier evaluations, transparency, and strict adherence to industry standards is necessary. Proactive identification, assessment, and mitigation of these risks are crucial for ensuring vehicle safety, security, and quality. Continuous monitoring and adaptation to emerging threats and vulnerabilities are vital for maintaining a resilient and secure supply chain.

9.4.Long Term (up to 2040)

9.4.1. Secure IoT Network through QKD and SDN

The advent of quantum computing will render conventional key exchange techniques such as RSA and Diffie-Hellman susceptible to compromise. To address the difficulty, novel methodologies rooted in quantum computing are being proposed. Quantum Key Distribution (QKD) is a cryptographic approach that leverages the quantum properties of photons to facilitate the secure transmission of cryptographic keys between several users. Quantum Key Distribution (QKD) networks exhibit a significant level of resilience against channel interceptions. A quantum key distribution (QKD) network will be constructed, consisting of one optical switch, two IoT gateways, and one IoT Server. The network will be developed in collaboration with ITMO, as illustrated in the accompanying diagram.

The suggested quantum key distribution (QKD) nodes are intended to be designed as supplementary cards that can be seamlessly integrated into the Internet of Things (IoT) Gateway and IoT Servers. The optical switches incorporated into the Quantum Key Distribution (QKD) network has Software-Defined Networking (SDN) capabilities, allowing them to be effectively governed and supervised by an SDN controller. A software-defined networking (SDN) enabled network stack will be created for the quantum key distribution (QKD) network, with the intention of deploying it in Internet of Things (IoT) gateways and servers. The deployment of the SDN controller application that supports dynamic channel selection and QKD routing is necessary within the SDN controller (scenario depicted in Figure 17).

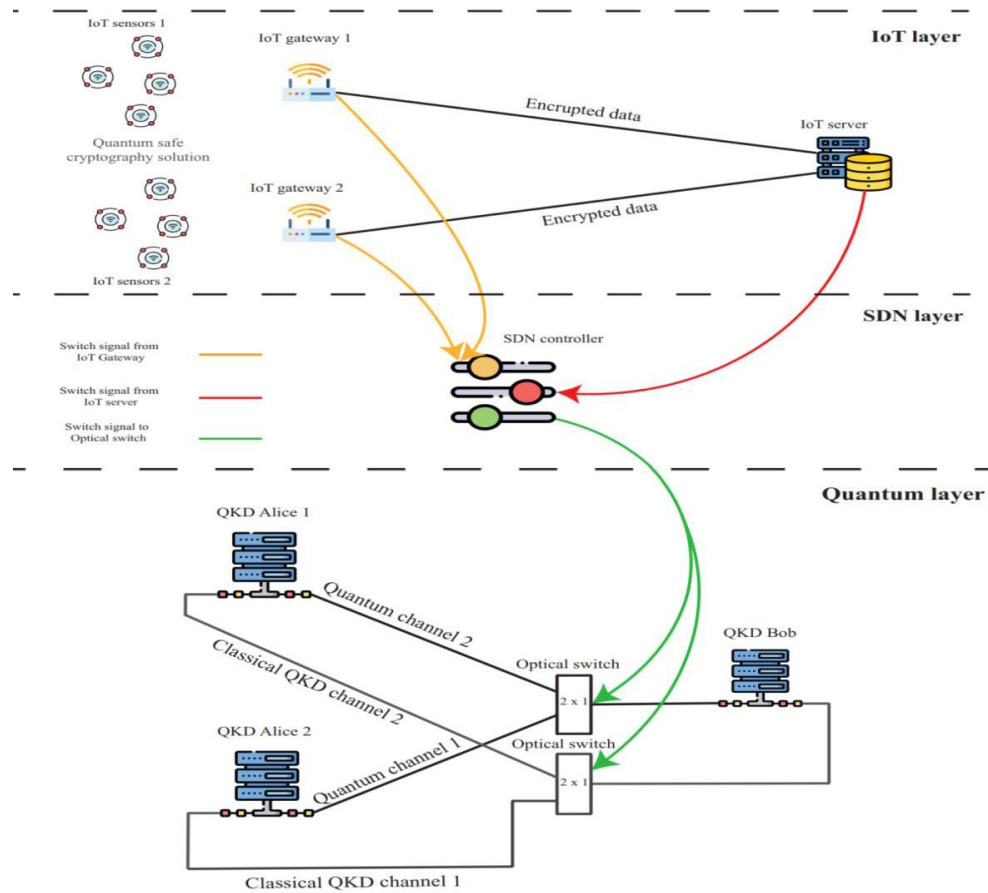


Figure 17: Quantum Communication with SDN and IoT

9.4.2. Federated Machine Learning and Swarm Learning

Thanks to the increasing maturity of federated learning solutions, the adoption of decentralized solutions for machine learning is increasing. One promising trend is to enable intelligence-based security in 6G by deploying a wide scale of decentralized mobile edge servers besides FL to detect and mitigate cyber-attacks in real-time. FL is a collaborative approach that enables performing the distributed ML techniques. It is a promising solution to provide security and privacy for IoT networks. FL shortens detection time, as the learning is executed locally. Besides it reduces communication overhead and bandwidth and takes full advantage of the edge's computation capability.

These solutions adopt techniques based on decentralized training that is then leveraged to centrally compute a model that. Essentially, the only parts decentralized of the machine learning lifecycle are the training part and the inference, while model computation and serving remain centralized. While it is a great step ahead in term of data privacy, data security, and reducing data transfers, it still requires an established trust between the parties involved, given that in the end the control of the whole machine learning lifecycle is centralized. To overcome these limitations, an new promising research direction is swarm learning, where learning occurs in a trustless and cooperative way based on pre-agreed rules (for example via ledgers and smart contracts). In the context of swarm learning, models are computed locally based on local data, without a central controller. Parameters are extracted from the models, shared across all the swarm nodes in a peer-to-peer fashion, and used to re-optimize local models. The research area in the domain of Federated ML/DL is still at its infancy but seems very promising to enable decentralized intelligent IoT solutions.

9.4.3. Self-aware IoT Protocols and its Security

Self-aware IoT protocols are networking and communication protocols used in the IoT that include mechanisms for self-awareness. With the help of these protocols, Internet of Things devices and networks may constantly assess their surroundings and adjust their own communication and behavior accordingly. Protocols on the Internet of Things that have self-awareness can improve performance, dependability, and safety.

Self-awareness IoT protocol is a notion in which IoT devices and networks may assess, adapt, and respond to security risks and vulnerabilities autonomously utilizing self-awareness and intelligence. It is a proactive approach to improving the security of IoT systems. Self-awareness features are built into IoT devices. They can detect anomalies or security breaches by monitoring their own activity, network traffic, and system characteristics. Monitoring power consumption, data traffic patterns, and gadget health are all examples of self-awareness. When an IoT device that is self-aware recognizes a potential security danger, it can take autonomous

activities to mitigate or respond to the threat. These procedures may include: disconnecting the infected device from the network, Implementing security procedures such as encryption or authentication Notifying a central management system or administrator, as well as Firmware or patches are automatically updated to resolve vulnerabilities.

Machine learning and artificial intelligence techniques are frequently used in self-aware IoT systems to continuously enhance their threat detection and response capabilities. These systems can adapt to and learning from previous security occurrences. Implementing self-awareness and AI in IoT devices will be difficult since they demand appropriate processing power and memory, which can be difficult for resource-constrained devices.

A centralized security orchestration platform can coordinate and control all self-aware IoT device security responses in the network. It may also collect and analyze data from many devices to detect global threats or weaknesses. To avoid unnecessary disruptions, it will be difficult to reconcile security with device performance. Security mechanisms must be resistant to attacks aimed at deceiving self-aware systems. Self-aware IoT protocols frequently include distributed decision-making techniques, in which IoT devices make decisions collectively to maximize network performance and resource allocation. Following are the proposed idea on self-aware IoT protocols and its security:

Create an IoT sensor network that is self-aware for environmental monitoring. The primary objective is to build a network of sensors that can modify their data transmission rates, power consumption, and data processing on their own depending on environmental circumstances. The sensors should be able to detect changes in their surroundings and alter their behavior, accordingly, ensuring resource efficiency and the collection of high-quality data.

Create an IoT healthcare monitoring system that is self-aware. It will concentrate on developing a system that can continuously monitor the health of patients or the elderly. Self-aware IoT protocols should be used by the system to adapt to changes in

the patient's health condition, adjust data transmission frequency, and provide alarms as needed. Machine learning should also be used for predictive health assessments.

9.4.4. Low power PQC

Designing an extra low-power post-quantum cryptography (PQC) system entails creating encryption and security mechanisms that can withstand quantum attacks while running efficiently on resource-constrained devices with restricted power sources, such as IoT devices or battery-powered sensors. The main goal is to create hardware acceleration for PQC algorithms to offload cryptographic processes from the CPU and therefore reduce energy consumption. Consider using low-power microcontrollers and platforms developed for low-power applications to operate them. Existing cryptographic processes within PQC algorithms can be optimized to reduce computational burden and power consumption. Exponentiations and modular arithmetic are examples of resource-intensive procedures that should be avoided. Create innovative sleep and wake-up cycle techniques for IoT devices to limit active periods and maximize low-power sleep modes. Create a system that only wakes up when necessary, such as when data should be encrypted or decrypted.

Design a low-power PQC solution for wearable devices and other health monitoring equipment. The major goal is to come up with a cryptographic framework that assures the privacy and security of health data collected by wearables while optimizing power utilization to extend the battery life of the device. To achieve longer battery life and lower power consumption for continuous health monitoring, the framework includes power-efficient cryptographic procedures and data transmission mechanisms. Similarly, different quantum-based cryptography methods can be enhanced or optimized, consume less power and operate more efficiently.

9.4.5. Low power to No power cryptography algorithm for IoT

Power consumption optimization in the design of cryptography algorithms for Internet of Things (IoT) devices is critical to promote efficient operation, extend battery longevity, and maintain performance in remote or demanding situations. To

reduce power consumption, it is critical to employ cryptographic algorithms that are specifically designed for resource-limited devices, with lightweight designs being prioritized. TinyCrypt, LowMC, and SIMON algorithms provide good security while having little computing overhead. The cryptographic operation can be offloaded to reduce power usage to nearly nothing. To move cryptographic functions from the central processing unit (CPU), it is recommended to use hardware acceleration on the microcontroller or System on a Chip (SoC) of the IoT device, if available. Hardware-based encryption and decryption techniques are usually distinguished by their high energy efficiency.

In cryptography algorithms, secure stateless operation means that each cryptographic operation does not rely on preserving a significant state between operations, which can lower the energy cost associated with state management. Various energy harvesting techniques, such as thermoelectric generators, piezoelectric harvesters, radio frequency systems, and vibration energy harvesters, have the potential to power IoT devices alongside conventional power sources, such as batteries. The use of this measure has the potential to result in a substantial decrease in power consumption. Energy harvesting for the IoT has emerged as a promising domain for research and development.

There are multiple ways for lower consumption of power and even attaining zero-power operation by implementing energy harvesting technologies. One of the primary objectives of IoT devices is to reduce power consumption during cryptographic activities, with the ultimate goal of achieving zero-power operation. There are multiple methods used to capture and transform various sources of energy from the environment into usable electrical energy that are referred to as energy harvesting techniques. These methods are intended to capture and use energy sources.

- Solar energy harvesting is the use of solar panels to catch and harness energy from the sun. Solar cells can convert light energy into electrical power, allowing IoT devices to operate and recharge their batteries.

- The use of vibration energy harvesters is proposed as a method of capturing mechanical vibrations and converting them into electrical energy. It is particularly useful in the context of IoT devices deployed in situations characterized by frequent vibrations.
- Thermal energy harvesting entails using thermoelectric generators to capture energy from temperature differences. Devices can convert thermal energy into electrical power, making them ideal for IoT applications involving temperature gradients.
- The capture and utilization of Radio Frequency (RF) energy produced from ambient wireless communications is the process of RF energy harvesting. RF energy harvesting modules can convert radio waves emitted by Wi-Fi, cellular networks, and other communication protocols into electrical power that can be used effectively.
- The use of piezoelectric materials to transform mechanical stress or vibrations into electrical energy is known as piezoelectric energy harvesting. It will be beneficial in harvesting energy from various movements or vibrations present in the gadget's surrounding environment.

Minimizing power consumption in cryptographic processes for IoT devices is a critical problem, with the goal of reaching zero power utilization. Cryptographic activities need the use of computational power, and the execution of such processes necessarily necessitates the expenditure of energy.

9.4.6. Deterministic Response for IIoT and Automotives

In the context of the Industrial Internet of Things (IIoT) and automotive systems, deterministic response refers to the ability of devices and networks to give consistent and predictable responses to varied events or inputs. Determinism is critical in domains such as industrial automation, autonomous cars, and real-time control systems that demand tight adherence to timing, reliability, and precision.

Important takeaways and real-world solutions of deterministic response in the IIoT and automotive are provided below:

Real-Time Control and Automation: In the context of manufacturing environments, industrial robots must conduct precise and accurate movements in response to sensor inputs or delivered commands. The use of deterministic response in robot operation ensures consistent task completion with low delay and high precision. Autonomous cars must be able to process sensor data quickly, such as lidar and radar, and then make quick decisions to maintain both safety and operational effectiveness. Deterministic control systems are critical to the safe navigation of many systems.

Low Latency Communication: The formation of low-latency communication among IoT devices is critical in industrial environments such as smart factories because it allows job coordination, equipment monitoring, and process control. Deterministic networking protocols are intended to offer data transmission and reception that is predictable.

Standardization: Time-Sensitive Networking (TSN) refers to a set of IEEE standards that enable deterministic communication across ordinary Ethernet networks, making it suitable for a wide range of IIoT applications. Automotive Ethernet protocols, such as BroadR-Reach, are used to enable deterministic communication within modern automobiles, allowing diverse applications such as entertainment and advanced driver support systems to run.

Consistency Across Heterogeneous Environments: The concept of deterministic response is critical in maintaining consistent behavior of devices and systems in the context of IIoT ecosystems, particularly in scenarios where diverse products from various suppliers are used in conjunction. Interoperability and consistency of behavior are critical in the automotive industry, especially when combining components and software from various sources.

Taking the aforementioned qualities into consideration, it is possible to build solutions targeted at improving operational efficiency and productivity in industrial

settings. The enhancement of safety and reliability in automotive applications, including self-driving cars. Reduced reaction times for critical processes have improved user experiences and increased system trustworthiness.

9.4.7. Zero Knowledge Proof

A Zero-Knowledge Proof (ZKP) is a cryptographic process in which a prover can demonstrate to a verifier that they have specific knowledge or capability without revealing the actual knowledge or capability. In essence, ZKPs make it easier to demonstrate knowledge while maintaining the confidentiality of the precise information being conveyed. ZKP offers the potential to improve privacy, data protection, and access control, hence minimizing the risk of information leakage. IoT systems can achieve a higher level of security while remaining efficient and privacy-preserving by implementing ZKPs.

ZKPs offer the potential to enable authentication of IoT devices while keeping their true identities hidden. A device instance can authenticate itself as an authorized sensor to a gateway without revealing its unique identification, so strengthening both privacy and security protections.

In cases where numerous IoT devices must exchange data, ZKPs can help these devices demonstrate possession of specified data without revealing the actual data itself. ZKP has the potential to be used in a variety of applications, including data marketplaces and collaborative sensing.

ZKPs have the potential to be used to validate the position of an IoT device while protecting the disclosure of precise GPS coordinates. The adoption of this technology has the potential to improve location-based services while protecting the privacy of the user's location information.


ZKPs have the potential to be computationally efficient, making them suitable for implementation on low-power IoT devices. This feature enables these gadgets to show evidence of specific features while consuming less energy.

Following are the potential research areas in the field of ZKP which can be used to design different IoT solutions.

- One such research area is the development of lightweight ZKP protocols appropriate for IoT devices with limited resources. This includes the creation of efficient methods for creating and validating proofs with low computational and energy costs.
- This research looks on hardware based ZKP accelerators, which aim to take the load of proof creation and verification off a device's core CPU, reducing energy consumption.
- This research investigates ZKPs that can dynamically adjust to the energy and processing resources available on IoT devices. The goal is to ensure optimal operational efficiency in a variety of environmental circumstances.






























10. Timelines: From Research to Mature Solutions

In the previous sections, we identified research, innovation and deployment priorities, emerging technologies, and trends to achieve trust, security, and privacy goals of IoT solutions. The table presents the recommendations and timeline of priorities over the period 2024-2040, highlighting the expected maturity and recommended priority for research, development, and deployment: research, technology development and field tests and pilot deployment. The table also reports the key technology enablers for each of the priorities. The timeframe has been selected, considering the scope of the upcoming work programmes as part of the new vision roadmap for Digital India. Obviously, taking into consideration the rapid evolution of digital technologies, timelines and priorities of the thrust areas and priority topics will require additional updates and reassessments in the future.

 Short Term

 Mid Term

 Long Term

Proposed Areas	Short Term	Mid Term	Long Term
5G and 6G Transition Security			
5G and IoT			
AI Enabled Botnet Detection and DNS Ecosystem			
AI Enabled Privacy and Data Protection			
Artificial Intelligence of Things (AIoT)			
Automotive Supply Chain Attacks – Risk Mitigation Strategies			
Blockchain assisted IoT Security			
Collective Intelligence: AI-Enabled Automotive Security and Threat Anticipation			
Deterministic Response for IIoT and Automotives			
Digital Twin			
Enhancement in the Automotive Security			
eSIM Cellular-IoT			
Federated machine learning and swarm learning			
High-performance computing (AI Capable) devices for the edge			
IoT Access Control			
IoT Device Certificate Lifecycle Management			
IoT Identification			
IoT Network Security Orchestration and Automation			
IoT Protocols			
IoT Security Sandbox			
IoT with IOTA Tangle Distributed Ledger			
Lightweight Cryptography			
Low power PQC			
Low power to No power Cryptography algorithms for IoT			
Low-power Quantum Random Number Generators (QRNG)			
MLOps and decentralized AI/ML pipelines			
New chip design and standards			
oneM2M			
PQC Enabled IoT Systems			

RISC-V based secure SoC for IoT			
Satellite Connectivity			
Secure IoT Network through QKD and SDN			
Self-adapting Intrusion Detection System			
Self-aware IoT Protocols and its Security			
Self-sufficient Intelligent Network (AI)			
Theft and Tampering of IoT Devices			
Trusted Components and Reusable Certifications			
UAV assisted Wireless Communication			
Zero Knowledge Proof			
Zero Trust Architecture			

11. Conclusion

As the global reliance on the IoT grows for information generation and gathering, it becomes crucial to establish and enhance international quality and integrity standards. It is necessary to guarantee the trustworthiness and traceability of data back to its original authentic sources. It is imperative to establish a strong collaboration between various standardization institutions and other global interest groups and alliances. The present document offers a thorough analysis and outlook on India's digital capabilities and technologies pertaining to a reliable and protected IoT framework. It encompasses several aspects such as data management, cybersecurity, artificial intelligence, skill development, interoperability, and others, both in the industrial and public sectors.

The identification of research, innovation, and implementation objectives and the corresponding issues to be addressed is crucial to provide guidance for future investments in both the public and private sectors. It encompasses tasks such as formulating forthcoming work plans and issuing requests for proposals. To adopt a critical perspective, it can be argued that the success of India's innovation strategy is contingent upon the effective implementation of a well-balanced amalgamation of people, infrastructure, and resources. To address the existing gaps in India's IoT innovation ecosystem, it is imperative for research institutions and important entities with expertise in the industry to take the lead in driving the nation's innovation agenda forward. To achieve the objectives of the Digital India vision and the becoming a USD 5 trillion economy, it is imperative for India to effectively design and implement a comprehensive national innovation strategy to foster a secure IoT ecosystem, thereby enabling the country to capitalize on the associated advantages.

12. References

- 1) IoT Analytics Link - <https://iot-analytics.com/number-connected-iot-devices/>
- 2) Grguric A, Khan O, Ortega-Gil A, Markakis EK, Pozdniakov K, Kloukinas C, Medrano-Gil AM, Gaeta E, Fico G, Koloutsou K. Reference Architectures, Platforms, and Pilots for European Smart and Healthy Living—Analysis and Comparison. Electronics. 2021; 10(14):1616. <https://doi.org/10.3390/electronics10141616>
- 3) IoT Cybersecurity survey. Link: <https://iot-analytics.com/understanding-iot-cyber-security-part-2/>
- 4) IoT Malware attacks statistics: Link- <https://www.sonicwall.com/2023-cyber-threat-report/>
- 5) IoT malware attacks up by 400% this year. Link- <https://www.businessinsider.in/tech/news/iot-malware-attacks-up-by-400-this-year-report/articleshow/104698771.cms>
- 6) ISO/IEC 30141. Link - <https://www.iso.org/standard/65695.html>
- 7) ISO/IEC 27402. Link - <https://www.iso.org/standard/80136.html>
- 8) ISO/IEC 27400. Link - <https://www.iso.org/standard/44373.html>
- 9) ISO/IEC DIS 27403. Link - <https://www.iso.org/standard/78702.html>
- 10) ISO/IEC 20924. Link - <https://www.iso.org/standard/82771.html>
- 11) NIST IR 8228. Link - <https://doi.org/10.6028/NIST.IR.8228>
- 12) NIST IR 8425. Link - <https://doi.org/10.6028/NIST.IR.8425>
- 13) NIST SP 800-53.

Link - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
- 14) NIST IR 8259 Series. Link - <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series>

- 15) NIST IR 8267. Link - <https://doi.org/10.6028/NIST.IR.8267-draft>
- 16) ITU-T SG 17. Link - <https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx>
- 17) ITU-T SG 20. Link - <https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx>
- 18) NIST SP 800-213 Series. Link - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf>
- 19) ETSI EN 303645. Link - https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- 20) IoTSF IoT Security Assurance Framework. Link - <https://iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf>
- 21) IoTSF Vulnerability Disclosure Best Practice Guidelines. Link - <https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf>
- 22) IoTSF Secure Design Best Practice Guides. Link - https://iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf
- 23) IEC 62443. Link - <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
- 24) TEC 31318. Link - https://www.tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20practice.pdf
- 25) LITD 17 (19140,19141, and 19143). Link - https://www.services.bis.gov.in/php/BIS_2.0/StandardsFormulationV2/doc_details_outside.php?ID=MTkxNDM%3D

- 26) IoT Policy. Link - https://www.meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20%281%29.pdf
- 27) TEC TR SN M2M 009. Link - <https://www.tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20IoT%20M2M%20Security.pdf>
- 28) IS 18004: Part 1. Link - https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/standard_review/Standard_review/Isdetails?ID=MjU4OTY%3D
- 29) ITU-T Y. 3056 Link - <https://www.itu.int/rec/T-REC-Y.3056-202102-P>
- 30) TEC 31328. Link - <https://tec.gov.in/public/pdf/M2M/Security%20by%20Design%20for%20IoT%20Device%20Manufacturers.pdf>
- 31) ITU-T Y. 3052. Link - https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3052-201703-I!!PDF-E&type=items
- 32) TEC 31188. Link - https://www.tec.gov.in/pdf/M2M/TR_National%20Trust%20Center_TEC%2031188_2022.pdf
- 33) TEC 93009. Link - <https://tec.gov.in/pdf/MTCTE/MTCTE%20PROCEDURE%20ver%202.1%20Release%200May%202021.pdf>
- 34) ITU-T Y. 4500.3. Link - <https://www.itu.int/rec/T-REC-Y.4500.3-202301-I/en>
- 35) Roadmap for Cybersecurity in Autonomous Vehicles <https://arxiv.org/pdf/2201.10349.pdf>
- 36) Ondrej Burkacky, Johannes Deichmann, Benjamin Klein, Klaus Pototzky, Gundbert Scherf. Cybersecurity in automotive: Mastering the challenge. McKinsey & Company (March 2020).

37) Quantum Sensors & IoT. Link - <https://ts2.space/en/the-impact-of-quantum-sensors-on-the-internet-of-things-iot/>

38) eSIM analytics. Link - <https://trendingtech.io/2021/04/08/can-sim-be-the-enabler-of-massive-iot-connectivity/>