Ministry of Electronics & Information Technology Government of India

सत्यमेव जयते

DSCI PROMOTING DATA PROTECTION A NASSCOM® Initiative

National Centre of Excellence Cybersecurity Technology And Entrepreneurship

CYBERSECURITY CENTRE of EXCELLENCE A joint initiative of DSCI & Government of Telangana

IoT SECURITY GUIDE

AUGUST 2022

Table of Contents

CONTENTS

Table of Contents

CONTENTS

Table of Contents

CONTENTS

EXECUTIVE SUMMARY

The Internet of Things (IoT), which will soon expand to the Internet of Everything, is a historical shift in the way we interact with our surroundings, our workplaces, and society. Our ability to converge the digital and physical worlds through IoT holds tremendous potential for the digital economy.

With the advent of 5G technologies, IoT technologies are set to take a giant leap forward. 5G can support a large number of static and mobile IoT devices, which have unique bandwidth, speed, and quality of service requirements. With these capabilities, we will see an explosion in IoT usage and innovation. In fact, as per an IDC report, IoT is expected to consist of more than 55 billion connected devices generating 80 Zettabytes of data by 2025. However, in addition to new opportunities, the IoT era also introduces new attack surfaces, which are already being exploited by cybercriminals.

While IoT promises to bring efficient business results across several industry verticals, organisations just focusing on connectivity to win the digital transformation race and putting security in the backseat would place the entire ecosystem at risk of fraud and attack.

In this context, we aim to present a wide spectrum of technological perspectives on IoT Security through our **IoT Security Guidebook**. This guidebook is a comprehensive document that covers IoT communication protocols as well as advice for building architectures for designing and developing IoT applications. Furthermore, the document highlights existing security architectures used across various industries. Threat modelling for IoT will assist developers in risk prioritization and lay the groundwork for establishing a product protection plan.

The purpose of the IoT Security Guidebook is to help the budding Internet of Things industry develop a unified knowledge of security challenges. The IoT Security Guidebook advocates for a methodology for designing secure IoT Services that ensures security best practices are followed throughout the service's life cycle. The documents offer recommendations on strategies to deal with common security threats and flaws in IoT services. It is intended to give a set of design recommendations for developing a secure product for IoT service providers. This document will operate as an overarching model for evaluating which features of advanced technologies or services are significant to the developer. Once these elements, or components, have been identified, the developer can assess the risks associated with each one and decide how to mitigate them.

Its scope is identified as design and deployment-specific recommendations for IoT services. It should be noted that national rules and regulations for a given territory may take precedence over the guidelines outlined in this document in some circumstances.

Key Takeaways

IoT is the network of inter-connected devices that can process data and communicate with each other, without the need for human intervention. IoT-based technology will deliver an advanced level of services in the coming years, effectively changing how people live their lives. Mobile computing, Pervasive Computing, Wireless Sensor Networks, and Cyber-Physical Systems are just a few of the categories where IoT is well-established. A few of the opportunities include new business models, diversification of revenue systems, real-time information and global visibility. The elements that shape the IoT ecosystems are Intelligent decision-making, communications, embedded systems, sensors and actuators. Advancements in Wearables, Smart Homes, Smart Cities, Smart Grids, Industrial, connected cars, Smart Retail, Smart Supply Chain, Smart Farming and Connected Health are a very few of the categorical examples of IoT use cases. This document outlines some of the prominent standard IoT network communication protocols such as Wi-Fi (Wireless Fidelity), Bluetooth, Zigbee, and 6LoWPAN (IPv6 over Low-power wireless personal area networks) and LoRaWAN (Long Range Wide-area network).

A significant proportion of IoT solutions designed for a specific application are dispersed and heterogeneous, making standardisation difficult. Security is one of the most important considerations for IoT, and it must be recognised alongside the overarching need for safety, as the entire world is closely intertwined with both concerns. The IoT Application Architecture gives detailed outline models and strategies for both design and development of an application. It also offers the readers a blueprint and recommendations to develop an application in a well-structured manner. The lack of technical standardisation in the IoT ecosystem exposes hardware, software, and relevant data to attacks and threats. It is therefore essential to dedicate more time to formulating industry guidelines and architectural standards required to efficiently implement IoT. Regulation of IoT products will be beneficial to improving the scalability, interoperability, security, and reliability of these products, especially given the complicated nature and uncertainty of the IoT ecosystem.

The document also underlines the Security concerns of IoT, since almost all IoT devices can threaten personal Confidentiality and public safety through cyberattacks. A few standard problems while tackling the security concerns include limited device resources, fragmentation of Standards and regulations, Security Integration and Data Privacy. The broad range of security concerns needed in IoT to enable design security, data protection, risk analysis and other concerns are outlined. The best practices to tackle these are by establishing secure IoT lifecycle guidelines on software and hardware development, Implementing role separation in Application Architecture and Supporting the establishment of IoT security strategies and Regulations.

The document also highlights the solutions among different Industries such as Huawei's IoT solution security architecture (the 3T + 1M framework), LTTS IoT Security Framework and Zero trust Architecture. The document presents the key components of LTTS IoT Security Framework and oneM2M standards and the benefits of using oneM2M.

The document presents several IoT Application architectures in focus such as,

- The Healthcare industry uses a bounded network with high integrity zone, a boundaryless network and a hybrid with different network technologies.
- Smart Home Ecosystem that uses Hub Architecture also addresses the security concerns of hub including device and software security.
- Industrial control systems are a broad category that includes DCS, SCADA as well as other PLCs used in Industries and essential infrastructures.

The document also highlights the solutions among different Industries such as Huawei's IoT solution security architecture (the 3T + 1M framework), LTTS IoT Security Framework and Zero trust Architecture. The document presents the key components of LTTS IoT Security Framework and oneM2M standards and the benefits of using oneM2M.

- Distributed Denial of Service (DDoS), provides types of attacks at different levels such as device level, network level and Application level.
- Hardware Security provides types of attacks on hardware such as side-channel Attacks, Rowhammer attacks, Hardware Trojan attacks, Physical attacks, Reverse engineering, Hardware IP Piracy, Mod-chip attacks and Security Architecture Attacks.

Hardware security issues arise when the vulnerabilities at different levels are not patched due to the lack of robust security for software and system. The document comprehensively outlines the Embedded system Hardware and Security, and the properties of securing an embedded system. A very minor vulnerability is required to create an exploit, to attack an embedded system. To achieve security, a list of properties of highly secured embedded systems is specified in the document.

The document gives a comprehensive understanding of the Data-at-rest Protection, which secures the data from unauthorized access.

The document states about the data layers that include,

- The hardware layer, the whole medium used for storage is encrypted by using FDE. It encrypts all the information including the hidden files.
- Block Manager Layer, the encryption is carried out at a higher level, the device-management layer, typically a block-oriented driver.
- The file system layer provides well-gross control over the selection of information that requires storage privacy.
- The application layer can add their data protection by using underlying file-system encryption features.

Information concerning secure boot and methods, Hardware resource partitioning, Software containerization and Isolation, Attack surface Reduction, least Privilege and Mandatory Access Control, Implicit Distrust and Secure Communication, Data Input Validation, Secure software development, build options and OS configurations, Integrity Monitoring and Auditing have been addressed.

A few of the Attacks involving Privacy violation and Data leakage Attacks in each of the layers is specified. Weak authentication Attacks, firmware Hijacking, Device scan Attacks, MITM attacks, Identity spoofing attacks, Malware injection attacks, SQL injection attacks, and Cross-site Scripting are just a few of the attacks associated with embedded system security and appropriate measures to prevent the attacks are presented.

The document exemplifies SCADA (Supervisory control and data acquisition) as they are a set of computing devices both software and hardware that work together to control a system. The main components of SCADA involve Supervisory computers, Remote terminal units, PLCs and Human-machine interfaces (HMI). Since SCADA networks are widely used in today's businesses to monitor and study real-time data, control industrial operations and connect with devices. As these systems are critical for industrial organizations, the need for SCADA security is essential.

Cyberthreats to SCADA and IoT Systems need to be comprehended, as these systems are usually used to manage Industrial Control Systems. Suggestions proposed by the President's critical infrastructure protection board in the United States to increase SCADA cyber security in protecting Industrial control systems have been stated. While securing the SCADA systems, the challenges to secure SCADA systems in IoT-Cloud Environments have been acknowledged. Advanced Persistent threats, Data Integrity, MITM, Replay Attacks and Dos Attacks are just a few of the threats to SCADA systems in the IoT-cloud context. The Best practices for securing IoT-Cloud-based SCADA systems are Network Segregation, Monitoring and Analysis, Log Analysis, File integrity monitoring, network traffic analysis, Memory dump analysis, Actively evaluating of security vulnerabilities, and Constant updating and fixing.

The threat model for IoT involves a Risk evaluation methodology which measures the relative importance of risk and helps organizations work on it. There are several forms of threat modelling and also how to carry out threat modelling by determining the trust boundaries, who the stakeholders are, the vital assets that must be safeguarded, attack surfaces, possible future risks and threats that have been detected are subjected to a risk assessment. Data-centric Threat modelling explains the combination of attack and protection side details for data of interest in a structured model that aids in vulnerability analysis, decision making, and change management in steps.

The document illustrates the importance of IoT Threat modelling with an Architectural IoT Threat Modelling Example which describes basic threats architecturally-based IoT hazard modelling. Threat modelling for Device-Level security describes different threat modelling methods, and their features and also gives an in-depth knowledge of each model with its frameworks. There are different types of threat models which target different IoT Networks which have different threats and risks which can cause different rates of damage. The document guides on identifying threats and providing security with risk mitigation by conducting assessments. There are millions of devices connected to the internet across the globe and there are several vulnerabilities they carry which could compromise users' data.

There is a lot of research and development ensuing in IoT Security in several areas. The key areas, their importance, technologies and challenges are described in this document. There are two different security standards covered in this document which are IIoT and IoXT. IIoT is used in manufacturing, supply chain monitoring, and management. IoXT has some rules and this document explains each of them in detail. There are IoT security standard protocols each protocol covers a different area but shares a common base of making IoT better on a daily basis. This document explains the importance of these protocols and how they support organizations by explaining their working models and functionalities.

The advent of 5G will connect all the citizens virtually through machines, objects, and devices. This document explains different technologies used in 5G, deployment and how they changed the phase of connectivity in IoT along with the security recommendations for 5G which explains vulnerabilities and attacks that can cause data thefts and also how can one avoid these by following different strategies, and security solutions to make a better 5G environment.

1.1 Evolution of IoT

The Internet of Things (IoT) is a conceptual paradigm that has emerged over the last few years. Kevin Ashton introduced the concept of IoT back in 1991. It describes a wide ecosystem where interconnected devices and services collect, exchange, and process data to adapt dynamically to a context.

Internet of Things (IoT): a wired or wireless network of uniquely identifiable connected devices that can process data and communicate with each other with or without human involvement.

IoT encompasses several fields of study, including Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and Cyber-Physical Systems (CPS). IoT represents a growing and changing field with many definitions.

The Internet of Things is tightly bound to cyber-physical systems and, in this respect, is an enabler of Smart Infrastructures by enhancing their quality-of-service provisioning. The IoT is the natural evolution of computing, and it brings its own challenges – an immature ecosystem plagued by fragmentation of standards and security concerns in a currently non-homogeneous IoT market because each industry and application are different. Another IoT challenge worth highlighting is its ability to scale globally. According to the IoT Analytics "State of IoT - Summer 2021" report, the global number of connected IoT devices is expected to grow 9% to 12.3 billion active endpoints and by 2025 the total number of IoT connections is predicted to reach 27 billion. Currently, there are different solutions available in the market through various manufacturers such as Google, Microsoft, Amazon, Apple, and Samsung, among others, many of which use their proprietary cloud service, protocols, and operating system.

The threats and risks related to the Internet of Things devices, systems and services are manifold and evolve rapidly. With a great impact on citizens' safety, security and privacy, the threat landscape concerning the Internet of Things is extremely wide. Hence, it is important to understand what needs to be secured and to develop specific security measures to protect the Internet of Things from cyber threats. Involving billions of intelligent systems and millions of applications, IoT will drive new consumer and business behaviours, which will demand increasingly intelligent solutions.

As per Fortune Business Insights, the projected growth of the global IoT market by 2028 is $1,854.76 billion creating several opportunities for vendors and companies looking to capitalize on IoT.

Examples of these opportunities include:

- New business models: New value streams for customers, with a faster response.
- Diversification of revenue streams: Monetizing added services on top of traditional lines of business.
- Real-time information: Capturing data about products and processes more swiftly, improving market agility and allowing prompt decision making.
- Global visibility: Making tracking easier from one end of a supply chain to the other.

Elements of IoT

The following points provide an overview of the different elements that shape IoT ecosystems, namely the Things in the IoT, intelligent decision making, sensors and actuators, communications, and embedded systems.

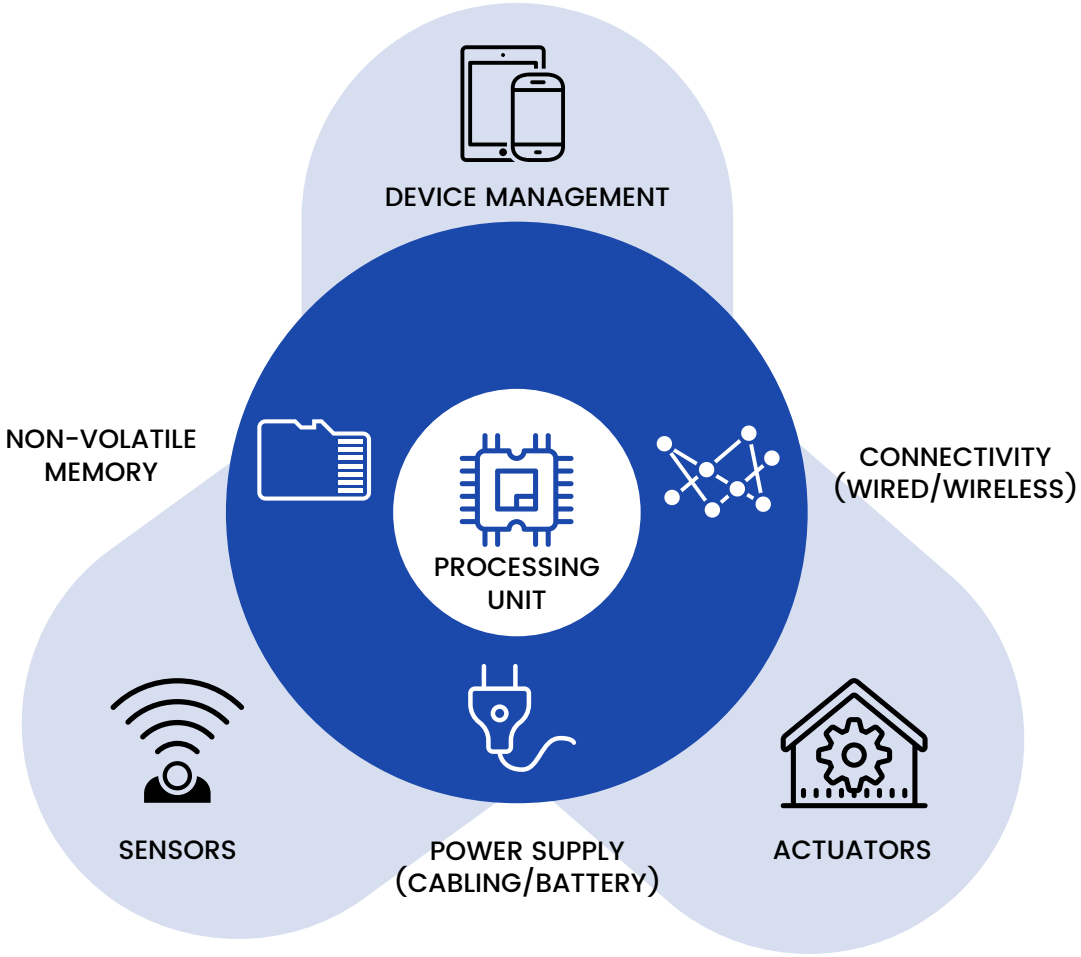


Figure 1. Structure of an IoT Embedded System

Examples of these opportunities include:

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLW, Wi-Fi, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Table 1. Indicative listing of Communication Protocols for IoT

1.2 Examples of IoT Applications

In this subsection, some examples of IoT applications shall be briefly presented.

Wearables

Wearable technology, sometimes referred to as "wearables," is a class of electronic devices that may be worn as accessories, attached to clothes, implanted in one's body, or even tattooed on the skin. The gadgets are hands-free devices with practical applications that are powered by microprocessors and can send and receive data via the Internet.
Wearable technology is considered an important section of IoT. Wearable devices are more prominent in the Healthcare sector. One example is the Fitbit. It helps us in maintaining a healthy lifestyle. It is a tracking device that helps track your sleep cycle, calories burned and tells us how much distance you travelled. Fitbit app also helps in viewing your key metrics such as oxygen saturation, skin temperature variation, Heart rate variability, resting heart rate, and breathing rate.

Smart Home

A smart home is a home with computer gadgets that allow for remote administration of appliances and systems like heating and air conditioning.
Due to IoT Home automation, home security measures have also evolved. Consumers may use their phones to watch CCTV security footage and operate their security systems from everywhere on the planet.

Smart Cities

Smart cities use IoT devices such as connected sensors, meters, systems, etc. to collect and analyze data. The cities then use this data to improve public utilities and services, infrastructure, and more.

IoT enabled smart cities' use cases spans across various areas like Smart Infrastructure, Air Quality Management, Traffic Management, Smart Parking, Smart Waste Management, Public Safety, etc.

Smart Grid

A smart grid is an electrical platform that allows for a two-way flow of electricity and data, as well as the ability to detect and respond to changes in usage and other concerns, thanks to digital communications technology. Smart grids are self-healing and allow power users to have an active role in the system.
IoT can be utilized in smart meters of the grids in order to measure various metrics like power consumption, network interoperability, etc., and also can help manage energy performance and power consumption.

Industrial

The usage of connected systems in industrial applications like automation, monitoring systems, and maintenance departments is termed as the Industrial IoT.

Connected Car

A connected car is a car that has an internet connection(owned), typically through a WLAN, which enables it to share the particular internet service and also the data associated with it, with other devices not only within the car but also outside the car.

Connected cars are linked to the network for enabling bi-directional communication among vehicles regulating the vehicle operations for enabling quick data transmission.

Smart Retail

Smart retail is a collection of smart technologies that are intended to provide consumers with a better, faster, and safer shopping experience. This revolution in retail has been facilitated by a society in which virtually everyone now carries a smart device – i.e., the smartphone.
Nowadays, consumers shop on their mobile devices and prefer products and services which offer discounts, faster delivery and a great shopping experience. Early adaptation of smart technologies by retailers can help them provide a seamless customer experience and ensure brand loyalty.

It is also possible to forecast **when** and **what** a client needs based on their purchase history, providing greater scope for targeted marketing.
IoT devices such as sensors are also being installed in teddy bears in hospitals to monitor the health of sick kids in a subtle and non-threatening manner.

Smart Supply Chain

Smart Supply Chain seeks to raise awareness for better decision-making by leveraging data from IoT devices and offering a detailed view of commodities and services from producer to store.
Clients may use Smart Supply Chain to automate not just shipping and delivery, but also to accurately anticipate product status in real-time and monitor key details that drive supply network productivity.

Smart Farming

Smart farming is a management concept that focuses on providing the foundation for the agricultural business to employ modern technology – such as big data, Internet of Things (IoT), etc. It is used to track, monitor, automate, and analyze activities. Smart farming, often known as precision agriculture, is controlled by software and monitored by sensors.
Smart farming is becoming more important as the world's population grows, as does the need for greater agricultural yields, the need to conserve natural resources and the growing need for climate-smart agriculture.
An example of a smart farming application includes temperature sensors which are used to scan the soil and control water, light, and humidity.

Connected Health

Connected health is an interactive-technical paradigm for managing and delivering healthcare that relies on technology to offer services offsite.
The Internet of Things (IoT) is a network of physical objects that employs connection to allow data to be exchanged. These gadgets aren't always the most advanced technological breakthroughs. They help healthcare professionals perform jobs more quickly by streamlining processes.

1.3 IoT Link Layer Connectivity

Several communication protocols are used in IoT to provide service to the network layer. The following are some of the prominent Standard IoT communication protocols.

Wi-Fi (Wireless Fidelity)

Wi-Fi is a local area network which is a wireless network proposed by Wi-Fi Alliance. Wi-Fi provides internet access to devices within a range of up to 100m. It uses high-frequency radio signals for sending and receiving data. It uses the IEEE 802.11 standard. The frequency and range of Wi-Fi are summarized in Table 3.
Wi-Fi data rate varies from 2Mbps (for Legacy 802.11) to 1.73Gbps (for 802.11ac wave 2). The quite common 802.11n has data speed up to 450 Mbps. We can set up PAN (Personal Area Network) or LAN (Local Area Network), or WAN (Wide Area Network) in IoT systems. By routing, we can increase the network area.

WI-FI PROTOCOL & SECURITY	802.11a/b/g/n/af
FREQUENCY	2.4 GHz, 3.6 GHz, and 4.9/5.0 GHz bands
RANGE	Common range is up to 100m but can be extended
EXAMPLES	Routers, Tablets, etc.

Table 3. Table Listing Frequency and Range of Wi-Fi

The data link layer within 802.11 consists of two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802 LANs, allowing for very simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLANs.

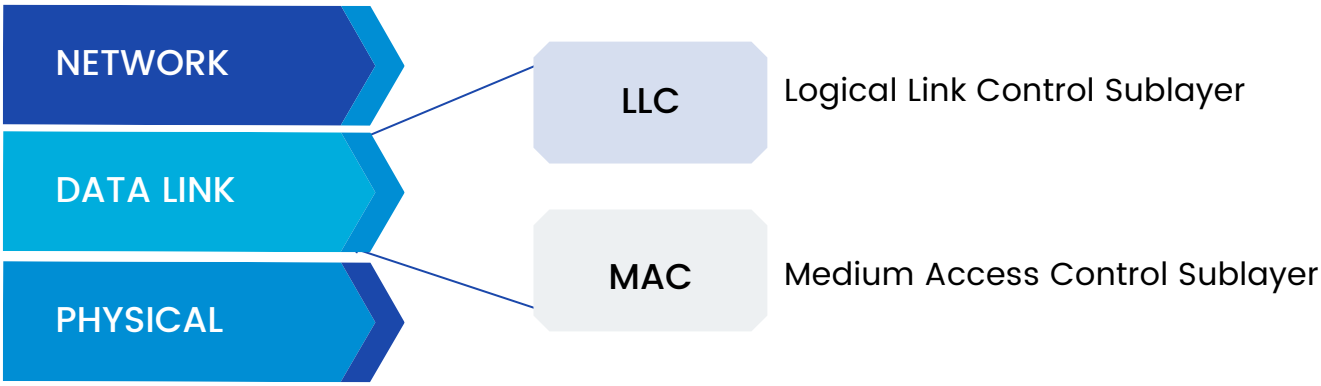


Figure 2. Data Link Layer

The 802.11 MAC is very similar in concept to 802.3 in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it. For 802.3 Ethernet LANs, the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol regulates how Ethernet stations establish access to the wire and how they detect and handle collisions that occur when two or more devices try to simultaneously communicate over the LAN.

The major drawbacks of Wi-Fi networking are latency and poor security. It is easier to hack a Wi-Fi hotspot and gain access to a physical link medium. However, a Wi-Fi network can be secured using WPA types and beacon packets management.

IEEE 802.11 provides for security via two methods: **Authentication** and **Encryption**. Authentication is the means by which one station is verified to have the authorization to communicate with the second station in a given coverage area. In the infrastructure mode, authentication is established between an Access Point (AP) and each station.

802.11 provides two methods of authentication: Open System or Shared Key. These methods are illustrated in Figure 3 and Figure 4. An Open System allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key authentication, on the other hand, requires Wired Equivalent Privacy (WEP) to be enabled and identical WEP keys on the client and AP (for more information on WEP keys, see below). The initiating endpoint requests a shared key authentication, which returns unencrypted challenge text (128 bytes of randomly generated text) from the other endpoint. The initiator encrypts the text and returns the data.

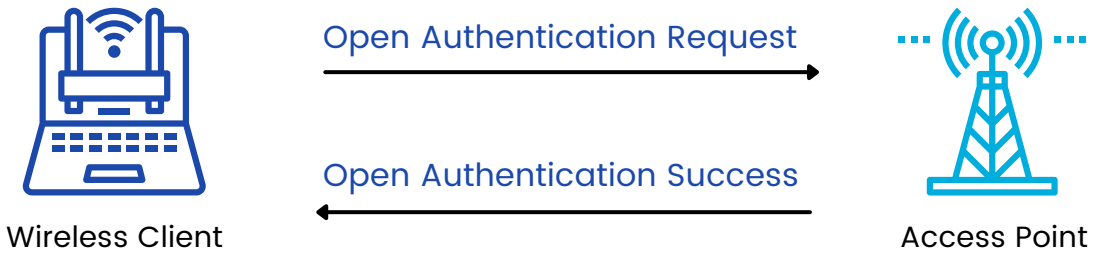


Figure 3. Open Authentication

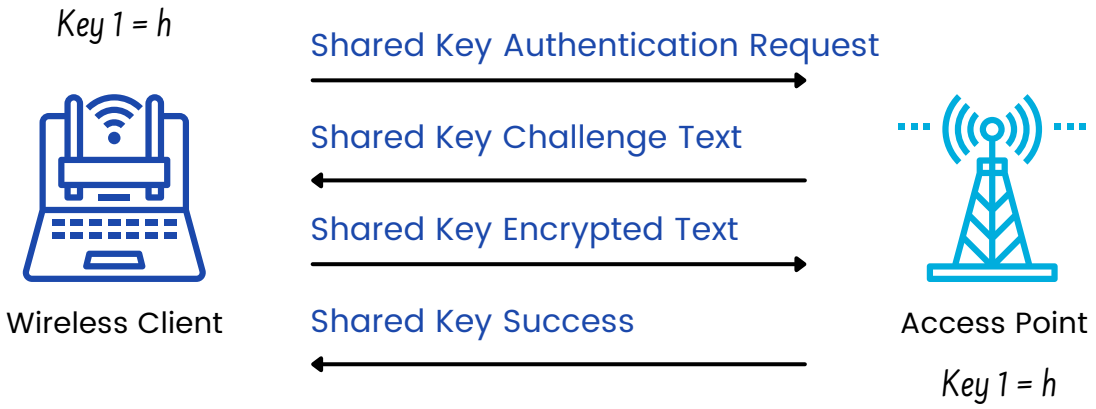


Figure 4. Shared Key Authentication

Encryption is intended to provide a level of security comparable to that of a wired LAN. The Wired Equivalent Privacy (WEP) feature uses the RC4 PRNG algorithm from RSA Data Security Inc. According to the protocol, WEP generally uses a 64-bit RC4 stream cypher (see information on 128-bit below). RC4 is a symmetric encryption algorithm, meaning the same key is used to encrypt and decrypt the data payload. This encryption key is generated from a seed value created by combining a 40-bit user-defined WEP key with a 24-bit Initialization Vector (IV). The WEP key generally takes the form of a 10-character hexadecimal string (0-9, A-F) or a 5-character ASCII string, which must be present on both ends of the wireless transmission. The protocol allows for up to four concurrently defined WEP keys.

The standard does not, however, currently define how the IV is established, so the implementation varies by vendor. When an encrypted wireless client starts transmitting data, the IV can start with a value of zero or another randomly defined starting value and generally increments upwards in a predictable manner with each successive frame. However, some vendors (such as Cisco) use a more sophisticated, random determination of the IV.

Although not yet part of the protocol specification, many 802.11b vendors also support 128-bit RC4 encryption. This requires a 104-bit WEP key (26-character hexadecimal or 13 characters ASCII) but uses the same 24-bit IV value.

Bluetooth

Bluetooth is a PAN (Personal Area Network), or it is a short-range wireless communication network for exchanging data between the connected devices through that network. It is economical in price and effective from a performance point of view for short-range distance. It is a 2.4GHz network that works well for personal wireless network communication. It provides a data transfer rate of 3Mbps in a range of 50m to 150m. Nowadays, Bluetooth is almost present in all smartphones, and it is highly used in wearable devices connected with mobile applications.

The Bluetooth Link Layer outlines the way Bluetooth devices can use the raw transmission facility given by the radio layer to exchange information. The link-layer characteristics of Bluetooth are summarized in Table 4.

MULTIPLE ACCESS SCHEME	TDMA
MAXIMUM PACKET SIZE	358 Bytes
ERROR CONTROL METHOD	ARQ, FEC
CHECKSUM LENGTH	1 Byte or 2 Bytes
IDENTIFIERS	14-bit public device

Table 4. Link Layer characteristics of Bluetooth

The functions of the Link Layer are very close to the MAC (Medium Access Control) sublayer of the OSI model. Functions of the Bluetooth Link Layer include:

- Defining procedures for discovering Bluetooth devices.
- Establishing logical links between the Bluetooth devices that are communicating. One of the devices is assigned as master, and the other is the slave.
- Broadcasting data to be sent. Managing the links between the devices throughout data communications.
- Sending data by converting the raw bit streams of the radio layer into frames and defining key formats.
- Considering the challenges of wireless transmission like interference, noise, and deep fades.

There are two main protocols in the link layer, namely, Link Manager Protocol (LMP) and Logical Link Control and Adaptation Protocol (L2CAP).

Link Manager Protocol (LMP)

LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.

Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP provides adaption between the upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.

Zigbee

Zigbee is similar to Bluetooth technology with a 2.4Ghz frequency. It is a low power personal communication network. It is cheaper and is widely used for several applications. It is used for specific commercial and industrial applications. Its range varies from 10-100m. The link layer characteristics of Zigbee are summarized in Table 5. Mesh networking is one of the important advantages of Zigbee technology. Zigbee supports star or mesh network topology.

MULTIPLE ACCESS SCHEME	CSMA-CA, slotted CSMA-CA
MAXIMUM PACKET SIZE	133 Bytes
PROTOCOL EFFICIENCY (RATIO OF PAYLOAD TO TOTAL PACKET LENGTH)	102/133 = 0.76 (76 Percent Efficient)
ERROR CONTROL METHOD	ARQ, FEC
CRC LENGTH	2 Bytes
LATENCY	<16ms (beacon-centric network)
IDENTIFIERS	16-bit short address | 64-bit extended address

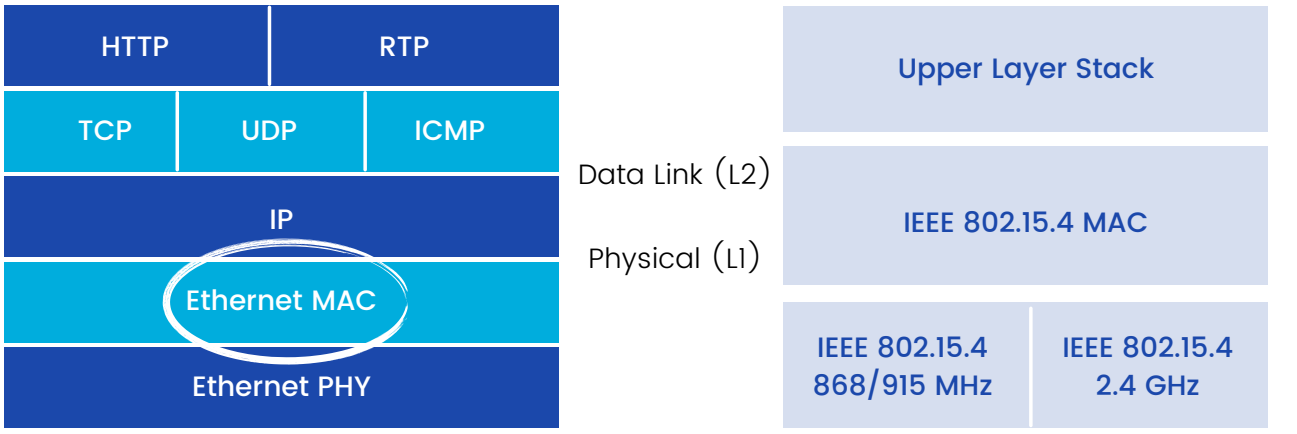
Table 5. Link Layer characteristics of Zigbee

6LoWPAN

6LoWPAN is an acronym for IPv6 over Low-Power Wireless Personal Area Networks (LPWAN). LPWAN is a wireless wide area network technology whose range varies from 2 km to 1000 km depending on the technology. The 6LoWPAN system is used for a variety of applications, including wireless sensor networks. This form of wireless sensor network sends data as packets and uses IPv6, providing the basis for the name, 6LoWPAN.

6LoWPAN has different features like support for 64 bit or 16-bit addressing, targeted at low power networks including Bluetooth low energy, header compression for IPv base as well as for UDP headers, network auto-configuration and neighbour discovery, support for multicast, unicast, and broadcast, supporting the concept of fragmentation. This makes 6LoWPAN the best-suited protocol for IoT.

Many low-power radio protocols are expected to use very small frame sizes. So, the frame size is dependent on the amount of payload or the data that need to carry and the amount of signalling data that is required to carry the packets. Figure 5 shows an example of a 15.4 standard frame where the payload, the actual user data, consists of 53 bytes whereas the total number of bytes to carry this packet is 127 bytes. One should realize that the addition of a header creates a fairly large amount of overhead.



(a) Link Layers and IP

(b) Link Layer: IEEE 802.15.4 for wireless

Figure 5. Link Layer of 6LoWPAN

LoRaWAN

LoRaWAN (Long Range Wide Area Network) is a wide area network protocol. It is a low power consumption protocol that targets wide-area network (WAN) applications with better security and mobility. It supports a large network with millions and millions of low-power devices deployed on public networks. It is a Media Access Control (Data Link or Network Access) protocol with some functions of the network layer also implemented. It is developed by LoRa Alliance. In this protocol stack, multiple end nodes (IoT devices) are connected to a gateway in Star Topology for M2M communication.

This protocol stack has been developed to cater to battery-powered IoT devices that need to connect wirelessly with a base station frequently. It is similar to Sigfox and Weightless technologies. The transceivers in this network typically have a coverage area of about 2 to 5 km in urban areas and 10 to 15 km in deep indoors. The IoT devices can communicate with a gateway at data speeds ranging from a few hundred bits per second to 50 Kbps.

2.1 Introduction

Application architecture outlines models and strategies for both the design and development of an application. The architecture offers you a blueprint and recommendations when developing an application to wind up with a well-structured application eventually.
Design patterns for software might help you develop an app. A pattern exemplifies a persistent solution to a problem. Instead of designing the architecture from scratch, you could use established design patterns and ensure that things operate appropriately.

Types of Application Architecture

Begin with your organizational plans when determining which application architecture should be used for a new application or even when examining your current architecture. Instead of picking an architecture and then attempting to adapt it to an application, you can simply design an architecture that will fulfil your interests. There are numerous application architectures, the most prominent of which are: Layered or N-tier, Monolithic, Microservices, Event-driven, Service-oriented Architectures.

Need for Application Architecture in IoT

Even though IoT solutions are designed using specialized techniques and associated with particular applications, the results are dispersed and heterogeneous and thus, not standardized. The prime reason is that the Internet of Things (IoT) is complex and nuanced. In IoT networks, the lack of technical standardization exposes hardware, software, and relevant data to threats and attacks. It is therefore imperative to spend more time in determining guidelines for industry and architectural standards necessary to implement IoT efficiently.
Without standards, we risk the possibility that technology will not accomplish its original purpose with a shorter timeline. Scalability, interoperability, security, and reliability are the fundamental advantages of IoT standardization.

2.2 Security Concerns of IoT

As we rely increasingly on smart, interconnected appliances in our lives, billions of "things" can threaten personal confidentiality and public safety through cyberattacks and external interference. Security is one of the greatest considerations concerning IoT, which needs to be acknowledged along with the overarching need for safety, as the physical world is intricately linked to both concerns. The regulation of IoT products, in particular given the complicated nature and uncertainty of the IoT ecosystem and considering scalability issues, is another important aspect.

The following standard problems have been recognized which impede the aggregation of more reliable IoT ecosystems:

Limited Device Resources

A significant redesigning of the existing IoT infrastructure may be required to execute standard security protocols because of technical limitations. Most IoT devices possess minimal computing capacities, memory, and power. Thus, advanced security measures cannot be easily implemented.

Fragmentation of Standards and Regulations

The fragmented and inconsistent development of guidelines and regulations to regulate the development of IoT security measures and best practices, as well as the rapid advent of novel technologies, complicate related concerns even further.

Security Integration

It is a very daunting task since the perspectives and expectations of those involved can contradict one another. For instance, various IoT devices and systems can be built on alternative authentication solutions, which must be integrated and interoperable.

Privacy Concerns/Data Privacy

- The best way to protect data is not to collect the data in the first place. Since non-essential data or data which is not needed to meet requirements simply puts privacy at risk.
- Responsibility for securing the data begins the moment we collect it, so it is always advisable only to collect the data that is required and ensure the protection of the collected data.

- The data collection should always begin with the user's consent. Even though the data collection begins with consent, it is necessary to provide protection to ensure privacy and the collected information remains confidential.
- For example, a patient health record should be only accessible by the patient and the doctor and necessary steps should be taken to ensure the protection of this data unless the patient provides consent to share.
- It is important to dispose of the data which is no longer needed and to achieve this, proper data retention and data disposal policies should be in place.

2.3 Security Recommendations

A detailed list of security measures and best practices to minimize the threats, vulnerabilities, and hazards reported affecting IoT devices and applications is described in this section. The security measures and guidelines for the various IoT contexts have already been established.
The first set of well-defined initiatives encompasses policies that typically aim to secure information and make it more comprehensive and robust. They should be acceptable for the operations of the company and should be well-documented. Security measures are indeed specified to tackle a broad range of security concerns, for instance, design security, data protection, risk analysis, etc.

Establish Secure IoT Lifecycle Guidelines on Software and Hardware Development

IoT products and solutions developers, sellers, and manufacturers should integrate and execute an SSDLC (Secure Software Development Lifecycle) for their IoT services and integrate related processes in their operations. At the application level and in each of the SDLC phases, security must be fully implemented. It is therefore important to empower more organizations to provide secure components for developers and end-users at the same time.
The theory of security and privacy by default and security and privacy by design is naturally the basis for IoT security. In IoT, cyber threats are perspectives (e.g., depending on the context of application), and this should consider the principles of security and privacy by design.
With such a focus on organizations, the incorporation of proper IoT security practices and well-defined and widely adopted tools (e.g., guidelines, checklists) would strongly support the default and design of IoT security.

Support the Establishment of IoT Security Strategies and Regulations

In terms of standardization, it is worth noting that the concept of the standard is acknowledged and endorsed by the industry, but diverse stakeholder organizations have distinct R&D chains, which ultimately adds to fragmentation. It is recommended that a set of best practices and guidelines for IoT security and privacy be established to overcome this fragmentation and this could be used as a benchmark for the implementation and deployment of IoT systems available in the market (for example- consult reports from AIOTI and ECSO). Each sector should subsequently concentrate on establishing specific policies, standards, and priorities depending on the specific context
and risk factors prevalent in each sector.

Implement Roles Separation in the Application Architecture

Every specific process must have a different user identity associated with the applications that run on an Endpoint. This assures that if an application is exploited, another application on the same Endpoint cannot be breached unless a second attack is successful. This additional phase taken by an Attacker is usually a severe obstacle to the overall exploit creation process, increasing the cost and severity of intervention against an Endpoint.
A custom privilege must be used for each application or service. In most scenarios, this is a separate user identity. Implementing separate user identities through the separation of roles means that if one service is breached, it cannot directly influence the assets used by another service within the same infrastructure. Secondary vulnerabilities must be identified in the local operating system to elevate privileges to exploit other services and users. This requires having a clear and solid application design that makes proper use of privilege separation.

2.4 Solutions Among Different Industries

Huawei's IoT Solution Security Architecture

For its IoT solutions, Huawei employs a "3T+1M" security architecture. The 3T+1M framework prioritizes security features at the machine, node, cloud, and application levels, all of which are aligned with one another. This might address security concerns in an IoT network at the sensor, network, and software levels. Huawei utilizes its comprehensive expertise in providing telecom network security guarantees to establish security situational awareness, examination, and surveillance for IoT, building on platform and cloud security. Huawei, in collaboration with other stakeholders, employs this architecture to effectively deal with the challenges of IoT security. Huawei is consistently optimizing its 3T+1M architecture to adapt easily to the security requirements of numerous industrial applications, especially industry-specific security specifications.

The 3T+1M IoT security solution focuses on the security of IoT scenarios (for instance, Connected Automobiles, LPWA, and Industrial IoT) by combining Three Technologies (3T) and One Management Approach (1M) to provide ensured support for IoT networks. "3T" corresponds to IoT device safety, network security assurance, and cloud protection technologies, while "1M" refers to security activity and management.

The framework focuses on ensuring consistency with local and international laws, as well as industry standards, while also providing end-to-end protection against online threats.

IoT Device Defense Technology Family (1T)

Offers IoT systems with compatible security features and device-cloud connectivity in a wide range of application scenarios. For weak devices, basic security functionality such as DTLS/DLTS+, trusted DICE, FOTA, and safe boot must be established (e.g., LPWA smart meters and shared bike locks). Security Certificate Maintenance, Intrusion Detection, Encryption Authentication, and a Trusted Platform Module (TPM) are needed for strong devices (e.g., vehicle-mounted T-Box and OBU).

IoT Network Assurance Technology Family (1T)

Identifies suspicious activity and imposes isolation, particularly for unusual IoT device behaviour. Unusual activity encompasses irregular traffic and reporting frequencies. For various circumstances, different IoT pipe security capabilities are improved. Anti-DDoS and signalling storm management capabilities, for instance, are enhanced for NB-IoT applications. The trustworthy functionality of V2X communication must be enhanced for Cooperative Intelligent Transport Systems (C-ITS) of connected vehicles.

IoT Platform Protection Technology Family (1T)

Outlines how to develop IoT platforms and clouds that would provide security situational awareness associated with big data analytics, awareness of connected vehicle and security analysis, and IoT data security and privacy protection. It also offers consumers configurable cloud security compliance capabilities.

IoT Security Operation and Management (1M)

Enables us to create E2E security maintenance resources, as well as how to build security operation and management requirements and procedures to enhance operational and testing performance. This also focuses on enhancing the IoT security framework in terms of threat detection and analysis, as well as response. Improved security testing tools, frequent IoT security assessments, automated system and application security monitoring tools, and threat intelligence libraries are all part of this.

Distinct IoT security techniques are used in various areas with the 3T+1M security architecture. Some concentrate on device security, others on network security, while others on cloud security. None of the other technologies exists in isolation; rather, they work together to form a robust security assurance framework. For instance, IoT devices must typically support a range of applications with limited resources, so device security capabilities must be integrated with those of the cloud and networks to enhance security at the edge.

LTTS IoT Security Framework

Conversations on privacy and cybersecurity threats in the implementation of Industry 4.0 have largely centered on the difficulties associated with the integration of Operational Technology and Information Technology. Nevertheless, considering the significance of connected systems in the manufacturing sector, Service Providers must transition to a Zero Trust Architecture (ZTA) as part of the industry 4.0 transition. This is needed for the systems that include external devices and services, such as IoT/IIoT and cloud services.

The LTTS IoT Security Approach allows suppliers and developers to easily switch toward more modern ZTA, improve security to existing infrastructure, or deploy sophisticated and advanced cybersecurity in new infrastructure.

Zero Trust Architecture

Zero Trust (ZT) is a security principle that requires auditing for any instance of accessibility, validating everything before granting access to information. ZT removes the risks associated with the conventional security strategy of supporting existing infrastructure implicitly (e.g., networks, devices, and users). ZTA is based on the authenticity of resources, limiting access to those who require it. Permissions are issued based on a security strategy of 'least privileges.'

By adhering to these guidelines, the LTTS IoT Security Framework implements Zero Trust Architecture:

- All sources of data, appliances, and applications are considered resources.
- Regardless of the network location, every exchange of information is protected.
- Specific resource access is provided on a per-connection basis.
- Until permissible access is granted, the resources are dynamically authenticated and strictly implemented.

Key Components of the Framework

The diagram below illustrates the LTTS IoT Security Framework's features that represent ZT concepts and are aligned towards the world of connected devices. These features fulfil the cybersecurity concerns of IIoT-connected devices and services.

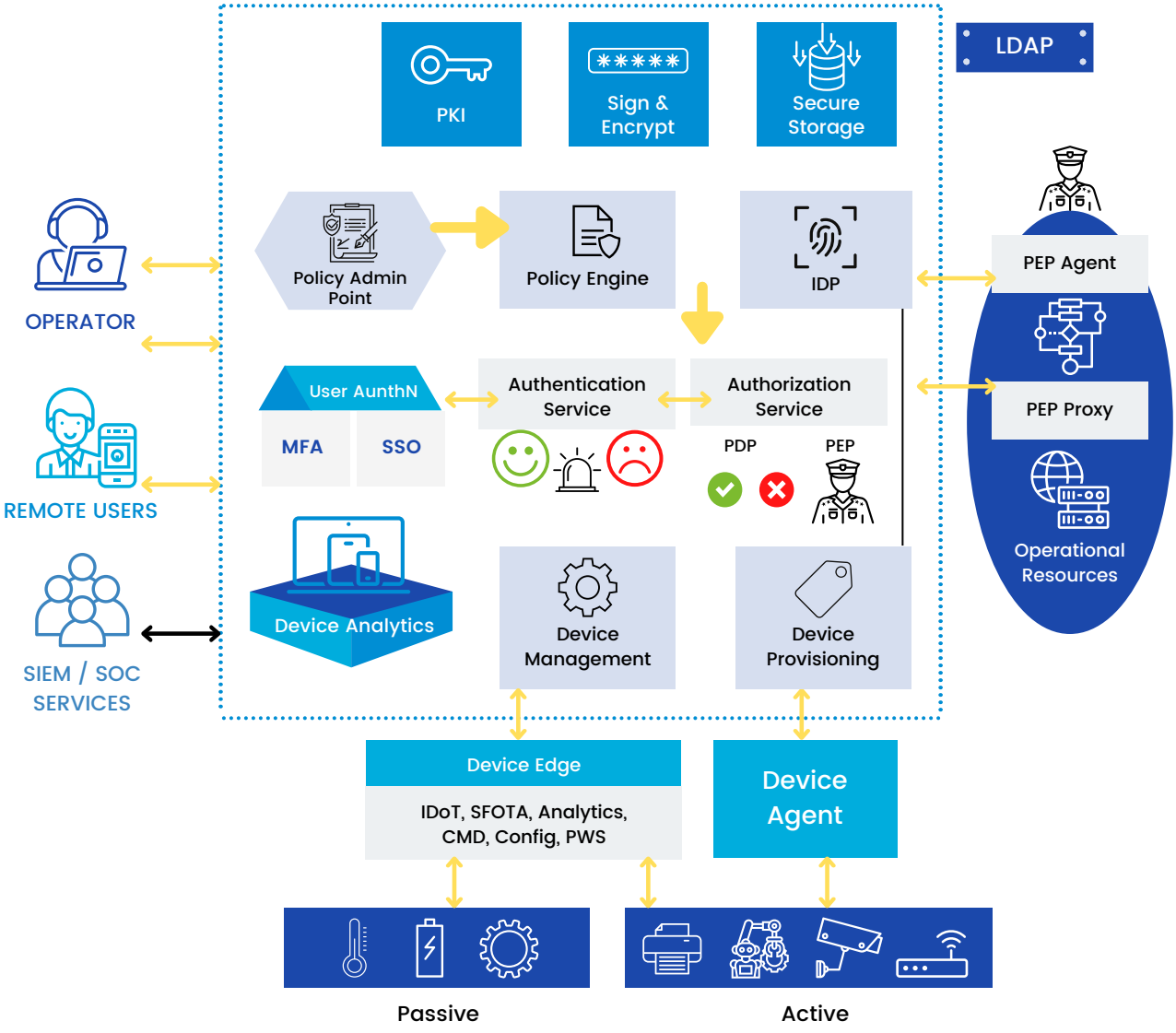


Figure 6. Source: "Industry 4.0: Transition to ZTA using LTTS IoT Security Framework," L&T Technology Services

With several elements, the framework performs the functionalities portrayed in Figure 6. Following the ZT concept, LTTS's Identity and access management (IAM) are fundamental to the security system, performing the essential functions of verification, authorization, and implementation. LTTS IAM gives the application owner a lot of freedom in establishing fine-grained authorization policies that are not restricted to predetermined use cases.

Benefits of LTTS Solution

- The LTTS strategy involves minimum attention in terms of integration.
- The approach is a mixed security solution that involves both cloud and on-premises protection.
- The framework is 'Cloud Agnostic,' which implies it provides full versatility and flexibility.
- The design is modular, which implies that additional safety modules can be incorporated at any time to meet new and complex needs.

---

oneM2M Standards

oneM2M is a global collaborative initiative driven by eight of the world's biggest ICT standards management organizations. The organization's mission is to develop a global technological standard for standardization in the areas of security, architecture, and API specifications for M2M and IoT applications dependent on specifications presented by its representatives.
oneM2M project is intended to be a long-term IoT deployment solution. These unified guidelines allow an Environment to enable a broad spectrum of applications and products, namely smart grids, smart cities, connected vehicles, smart homes, and healthcare. Perhaps one of oneM2M's priorities is to promote and start engaging organizations from M2M-related market domains like automation, navigation systems, healthcare, enterprise projects, home automation, and so on.
This is an open and accessible standard with transparent project development. At oneM2M, you can find all the regulations, including the drafts. oneM2M reportedly has over 200 partners involved.

oneM2M Overview

oneM2M Service Layer:

The oneM2M graded architecture describes an IoT Service Layer, which is a software interface that sits between processing/communication hardware and IoT applications and provides a valuable collection of features required by many IoT systems. It facilitates safe end-to-end data/control transfer between IoT devices, as well as authentication, authorization, and encryption.

The Service Layer of oneM2M is usually introduced as a software layer that sits among IoT applications and services that allow data storage, processing, and transport, usually on top of IP. Non-IP transports, on the other hand, are assisted by interworking proxies. The oneM2M Service Layer delivers functionality that is usually needed for IoT applications across various industrial sectors.

Horizontal Architecture

The Service Layer of oneM2M is usually introduced as a software layer that sits among IoT applications and services that allow data storage, processing, and transport, usually on top of IP. Non-IP transports, on the other hand, are assisted by interworking proxies. The oneM2M Service Layer delivers functionality that is usually needed for IoT applications across various industrial sectors.

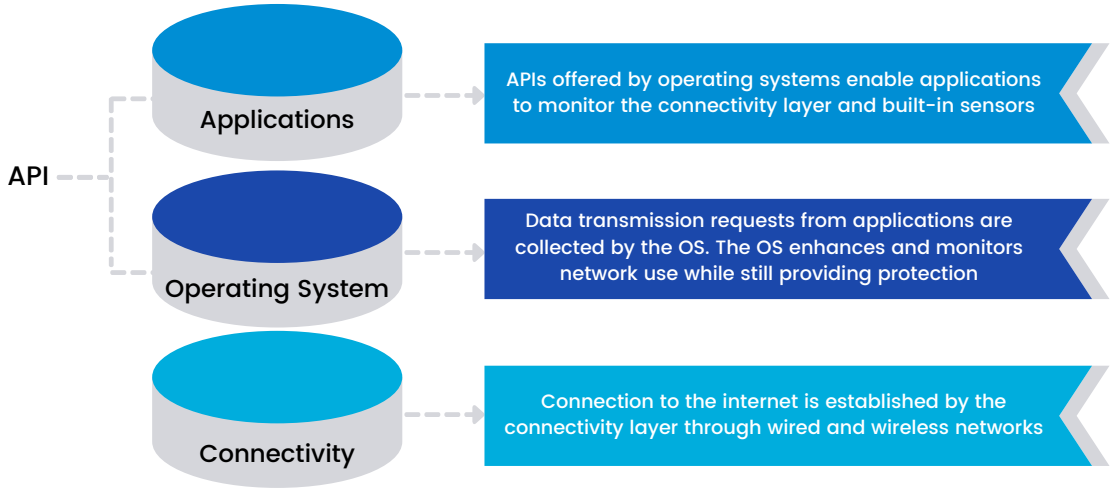


Figure 7. oneM2M's Service Layer

Functional Architecture

The oneM2M Layered Model is made up of three layers: the Application, the Common Services, and the underlying Network Services

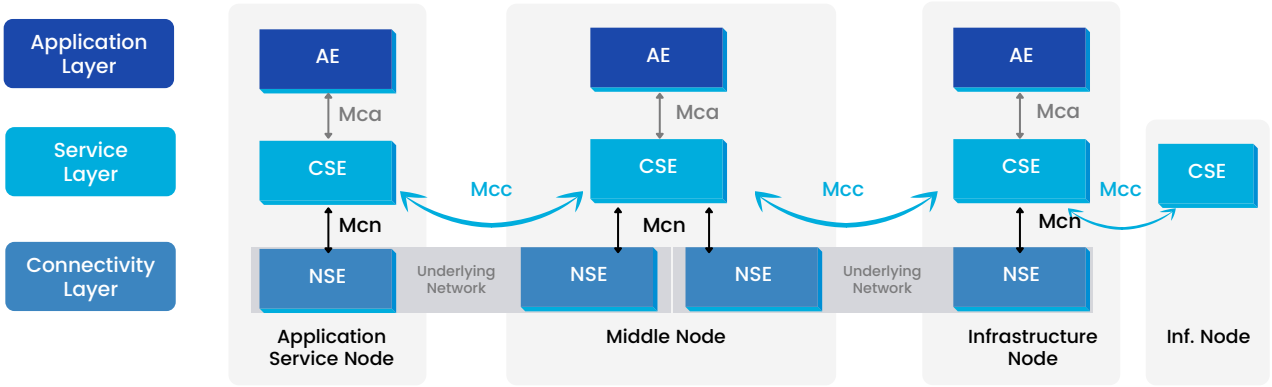


Figure 8. oneM2M Layered Model

(Source: https://www.onem2m.org/getting-started/onem2m-overview)

oneM2M Entities:

The following functions are defined in the oneM2M functional architecture:

Application Entity (AE)

It is an entity in the application layer that executes M2M application service logic. Each instance of application service logic execution is referred to as an "Application Entity" (AE) and is distinguished via a unique AE-ID. Examples of AEs include a vehicle monitoring application, a remote healthcare application, and so on.

Common Services Entity (CSE)

It is an entity that involves several oneM2M specified common service functions that can be utilized. The Mca (visibility to AEs) and Mcc (visibility to other CSEs) reference points reveal those service roles and responsibilities to other entities. Another reference point is Mcn which is used to gain access to the underlying Network Service Entities' services. Each CSE is distinguished via a unique CSE-ID. The CSE provides service functions such as data storage and sharing with access control, authentication, system management, and so on.

Network Services Entity (NSE)

This entity offers services to the CSEs from the underlying network. Location services, system triggering, long sleep cycles, and so on are examples of such services.

Benefits of Using oneM2M

The benefits of using oneM2M are as follows:

- To avoid platform or cloud provider lock-in, it uses open standards.
- There are several open-source implementations accessible (CSE or AE).
- Static and dynamic access control offers complete security at both the channel and object levels.
- The ability to easily interoperate/integrate with established and developing configurations lays the groundwork for long-term evolution and a sustainable future.
- Utilises the network infrastructure of the operators as well as current operational technologies.
- It is incredibly flexible because it can be integrated across all domains and is not restricted to a single protocol technology.
- Supported routing protocols and message serialisation can alter, but the oneM2M code will still not. This facilitates easy modification to future technological advancements.
- The horizontal platform enables multiple IoT domains by providing common service functions.
- Cross-domain innovation enabled by a unified methodology and standard APIs enables the exchange of information and processes across previously isolated domains (for instance, home security system vs heating system), aids in the development of new opportunities.
- The design of data-oriented RESTful API results in effective data sharing and semantic interoperability.

2.5 IoT Application Architectures in Focus

Privacy cannot be viewed as a bonus to current goods and services. Since decisions made in the digital world have a direct impact on the physical world, security must be built into services from the ground up to make sure that every action is permissible and every identity is validated as well as ensuring that these activities and the related meta-data are not disclosed to unauthorized parties.
The healthcare industry, transportation solutions, power grids, smart homes, surveillance systems, and other technologies have a significant effect on individuals' physical lives. It is the engineers' responsibility to maintain these goods and services to the highest degree of assurance possible, reducing the possibility of potential damage as well as the disclosure of private information.

Focus 1: Healthcare Industry

This section details technological and network frameworks tailored to the health sector to develop an awareness of potential risks and high-level thinking about securing healthcare systems and medical information from multiple threats. One such threat may be personal devices that share data with healthcare providers. We hope to encourage the best solutions for health-related IoT systems by considering these architectures for several devices and their security issues.

Reference Architectures

This section introduces three network topologies ("bounded," "boundaryless," and "hybrid"), as well as an environment map and network architecture about each. The following network topologies are briefly outlined in the subsequent lines.
A "bounded" network topology has a fixed boundary amongst network zones, which can be deliberate or unintentional, like access points between protected networks or even a bridge between connectivity. This architecture is especially applicable to fixed IoT healthcare products and some portable device use cases.
A "boundaryless" network topology has no fixed operational internal network or security safeguards. End-to-end security frameworks are thus needed. The use of the trust boundary to ensure permitted access facilitates data security and credibility. This topology is especially relevant to portable IoT healthcare systems and some individual device use cases.
A "hybrid" network topology can involve a mix of network technologies and topologies, such as bounded and boundaryless networks. This topology is especially pertinent to portable and personal healthcare devices.

Bounded Network with High Integrity Zone

A boundary could be an ideal location for implementing protective measures like traffic controls. Using boundaries to distinguish networks facilitates the protection of sensitive resources. It also encourages better information management practices and adheres to data protection laws by putting additional regulations in place for patient information.

Using boundaries can serve to minimize cyber threats and enhance organizational management. Boundaries that occur as a consequence of different network technologies may serve as a bridge between bounded regions or other network technologies, facilitating interoperability.

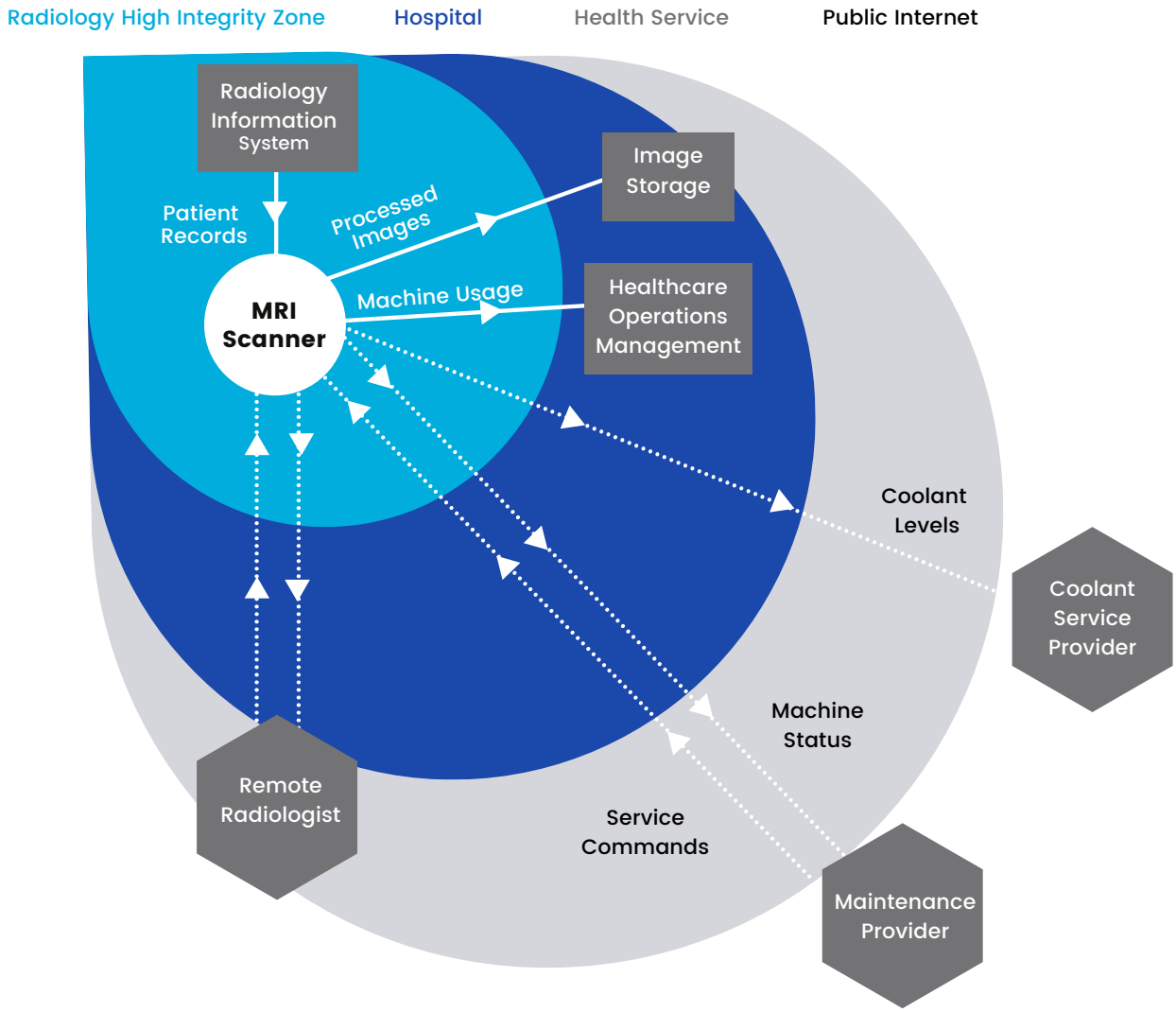


Figure 9. Source: "IoT Security Reference Architecture For The Healthcare Industry," IoT Security Foundation (IoTSF), 2019

Figure 9 depicts multiple nested regions, with the radiology department's critical systems residing in the innermost high integrity region. This is stored inside the hospital's internal network and is part of a larger healthcare network. Data is also sent to the public Internet for collaboration with external system maintenance and service providers.

Boundaries enable strong network security services to be deployed at points of interconnection. Boundaries often help to provide layered protection in an environment with a wide range of devices with diverse capacities and criticalities. For instance, if a section of a network is breached, a security gateway can fulfil the demand of critical devices by protecting the high integrity zone and its devices with low or weak security capacity from cyber risks.

The following are some examples of security management features that can be applied at network boundaries:

- Segregating internal and external networks to safeguard against potential attacks and facilitate monitoring and traffic segmentation as required.
- Isolating local networks into multiple network zones to better handle safety depending on the needs of that zone and to reduce a network's attack surface (e.g., protecting a high-integrity zone).
- The capability of sending warnings and updates in the event of an anomaly.
- The authority to grant permissions to a device or a group of devices.

Boundaryless Network

A Boundaryless Network illustrates the significance of services such as user authentication and monitoring updates. This is being accompanied by an escalation in the adoption of Web cloud infrastructure, which offers price and efficiency benefits while optimizing IT services. Similar developments can be observed in the healthcare industry, where there is a growing willingness to provide care to patients outside of a conventional hospital or clinic setting by utilizing cloud computing.

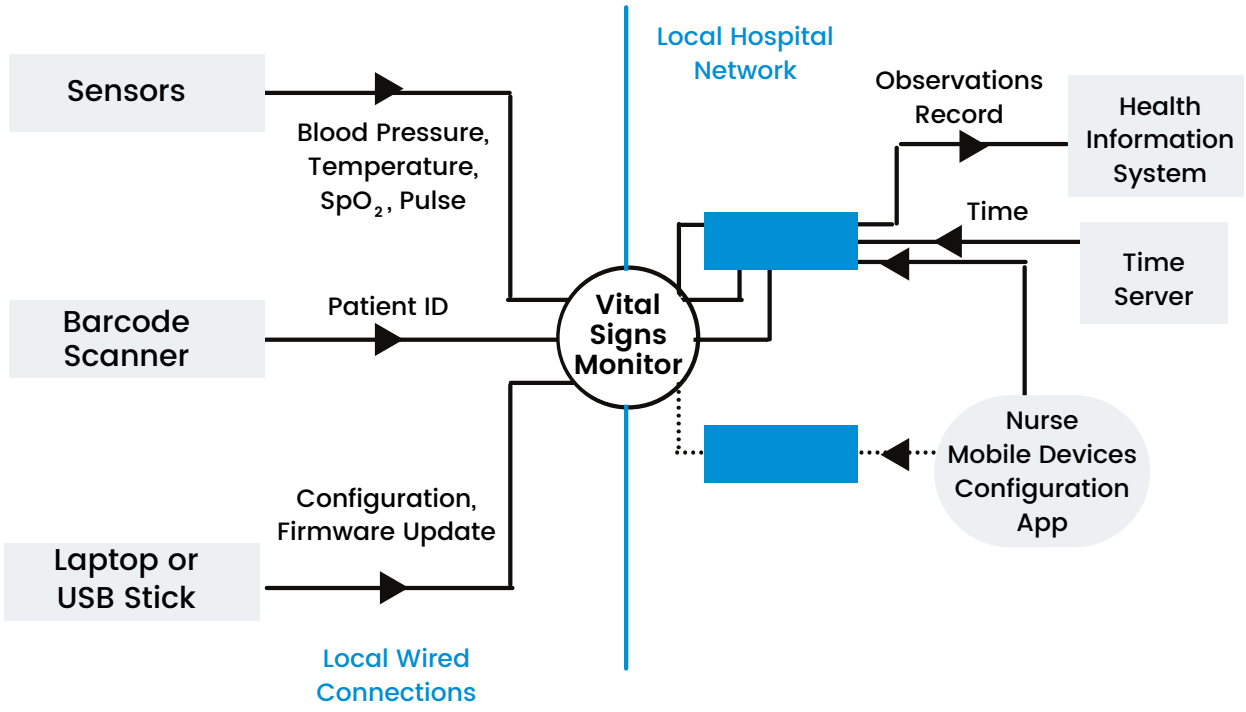


Figure 10 Source: "IoT Security Reference Architecture For The Healthcare Industry," IoT Security Foundation (IoTSF), 2019

Figure 10 depicts three separate networks – local wired or Wi-Fi, as well as public Internet – that can link healthcare equipment such as a vital signs monitor or a nurse's smartphone. In essence, this is a boundaryless network architecture in which communication will occur end-to-end over the Internet while often switching between networks. For example, the display is portable and can be connected to any accessible Ethernet port or connected to public Wi-Fi. When "on-site," the nurse's mobile device can be able to connect to public Wi-Fi or use a cellular link and thereafter connect to the hospital network when operating locally.

The following are some examples of security management functionality that could be incorporated at security management points:

- Organise authentication procedures.
- Keep your authentication credentials secure.
- Cover variety levels of authentication such as single token, server, and so on.
- An authorisation tool can issue warnings if an authenticated system has tampered with or unauthorised acts are being attempted.

Hybrid with Different Network Technologies

It should be noted that not all IoT health information is transmitted over IP-based networks. As a result, it is critical to understand how various network technologies can interact in this environment. This topology is especially applicable to portable and personal healthcare products with the following example architecture focusing on a personal device use case (connected hearing aid).

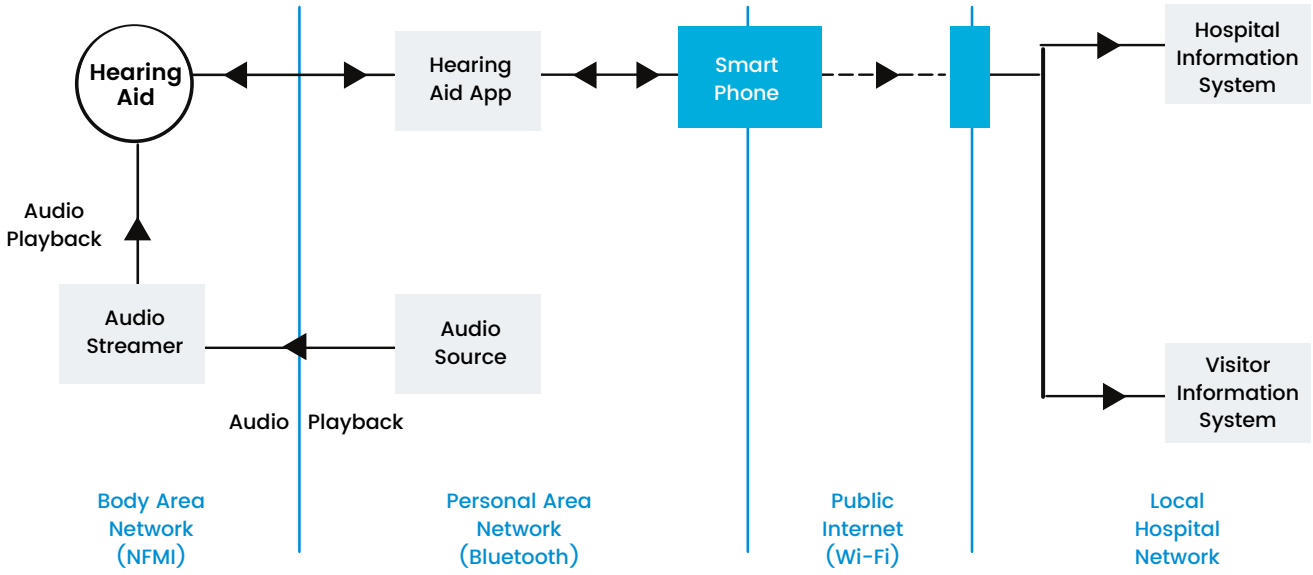


Figure 11. Source: "IoT Security Reference Architecture For The Healthcare Industry," IoT Security Foundation (IoTSF), 2019

Figure 11 depicts a framework using three separate network technologies: IP over the Internet, a Bluetooth Personal Area Network (PAN) with several profiles (excluding IP), and a Body Area Network (BAN) with Near Field Magnetic Induction (NFMI). These are depicted as three regions on the diagram. The regions in this example are used to demonstrate the network technologies that the various appliances and services in this hybrid network use to communicate with one another. Nevertheless, it is worth remembering that neighbouring regions may not always have a definite boundary. The hearing aid could be completely exposed to the PAN, and the hearing aid App may be completely exposed to the Internet. Moreover, because there is no direct routing between the BAN and the Internet, the hearing aid is not explicitly exposed to the Internet, and hence this is not a truly boundaryless network architecture.

The following are some examples of security management functionality that could be incorporated at security management points:

- Monitoring and auditing capabilities for analysis.
- Adding anti-virus/malware services in place.
- Applications are updated or patched.
- The privilege to revoke authentication and authorisation to pass ownership (for instance, maintaining device whitelists and blacklists).

Focus 2: Smart Home Ecosystem

Hub Architecture

This hub reference architecture intends to deliver user-friendly centralized security solutions for homes implementing IoT systems and technologies, particularly because this usually involves devices from multiple manufacturers. Specifically, the design prioritizes protection and offers a path forward with that in mind. This Hub Architecture, in contrast to other IoT architectures, offers a more reliable and straightforward home IoT ecosystem. By providing tools such as alarms and troubleshooting, the Hub architecture allows home IoT administrators to easily monitor and control their IoT environment.

It is also suggested that home IoT devices link to a dedicated IoT network rather than the personal residence network system for added security. For example, a router can easily and intelligently divide the home broadband into two networks: one for regular internet usage by occupants and the other for IoT devices like LEDs and smart assistants. The goal is to reduce the cyber threats to home IT and IoT networks by securing home network events from IoT devices that could be used as an easy target.

Example of Hub-based Architecture

The Hub framework is outlined here within five components. First is a schematic of the Hub architecture that indicates how the Hub is linked to other connected devices and security features. This is accompanied by three major procedures and their security requirements for IoT solution design and operation, namely Network Management, Connecting Devices, and Lifecycle Management.

Finally, a brief overview of security concerns for the Hub itself, including device and software security, is given.

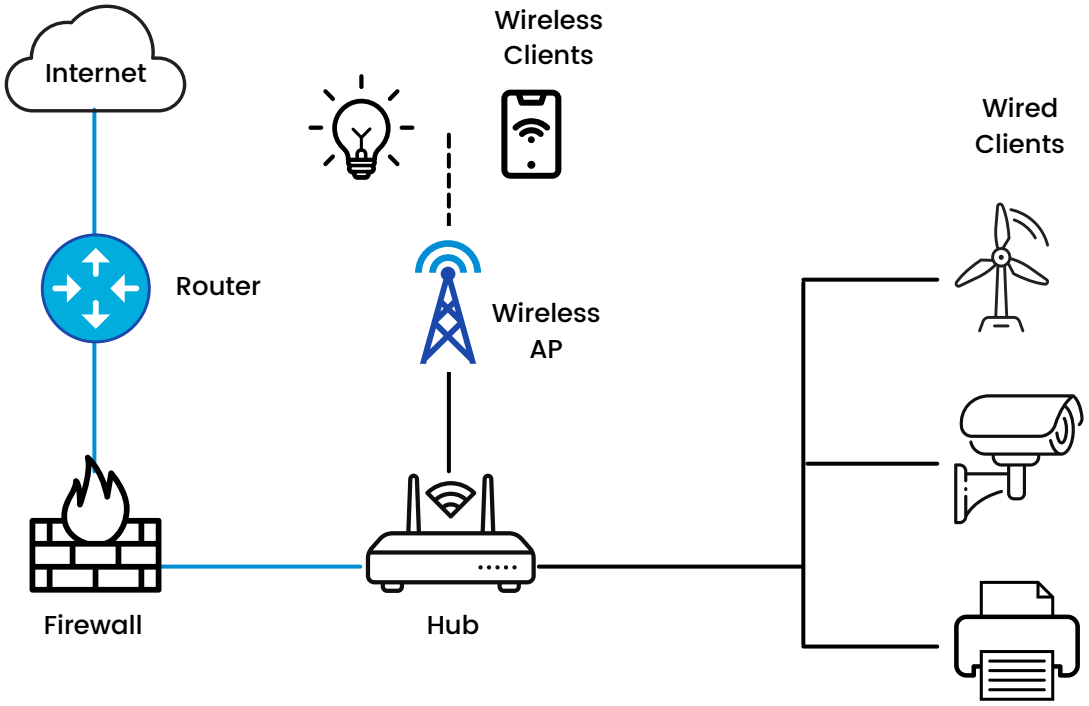


Figure 12. Source: "IoT Security Architecture and Policy for the Home - a Hub Based Approach," IoT Security Foundation (IoTSF), 2018

Figure 12 illustrates the multi-layered communication framework in a home IoT environment, reflecting the complex communication mechanism between devices, networks, and the centralized Hub. The router and firewall functions are shown separately, but they could also be integrated into the Hub along with other network functions, especially in those designed for homes with a limited number of devices. Devices (connected by grey lines) use this network to communicate with one another, with the Hub, and likely with external elements through a Hub gateway. The Hub, which gathers data and interacts with other architectural features like appliances and local networks, is at the heart of the IoT. Simultaneously, the Hub can act as a gateway to external home networks as required through its link to the firewall (blue line).

Network Management

Homes operate in several network configurations. It is best to practice for this architecture to have one dedicated network for IoT systems that uses local web access. A Hub could help with this by segmenting the home "IT" network. The "local IoT network" is thought to provide an additional layer of protection to both the devices and the home by isolating IoT device functions from the home "IT" network in the event of a data breach or breakdown. Nevertheless, not all Hubs can support network segmentation, and it is known that not all homes would be able to set up and maintain two local networks. Hence, security features should be integrated into IoT solutions to allow for a wide range of network architectures while maintaining a high level of security.

Connecting Devices Securely

The reliable authentication of an IoT device's authenticity and technology is essential in ensuring that only authorized and trustworthy devices are installed in the home. Authentication is the procedure of confirming that an item (or individual) is all it claims to be or that data came from the source reported to be its origin. An authorization manager, like the home IoT administrator, will authorize the system to operate on the network once it has been authenticated.
Inside a home setting, a Hub may have to handle authentication and authorization elements like identifying and logging devices, validating changes, and maintaining certificates without human intervention. As a result, the Hub must be able to merge data from several sources, including the IoT service provider, appliances, and home users. In a home, a hub should be adaptable not only in terms of technology or design but also in terms of home user ability.

Lifecycle Management

Regulating IoT system devices, networks, infrastructure, and efficiency is an important aspect of IoT security. Auditing data and analytics can be aggregated in a centralized location for improved visibility and control of the IoT system. A Hub serves as the main source of knowledge about the functioning of the IoT ecosystem for either the home IoT administrator or the service provider. With the rapid advancement of deep learning and big-data analytics, the home IoT administrator would be able to take appropriate measures, such as consulting a solution provider or taking a system offline and making intelligent choices based on what is obtained from the Hub's surveillance and tracking tools. This includes knowledge extracted from other security tools, including firewalls, gateways, and network access controls.

Hub Device Security

Since the Hub is desired to be a vital component of the home's IoT security, it should have robust security. This includes features like:

- Potential to safely store confidential information such as roots of trust, safety requirements for website & mobile user interfaces, along with network connections.
- Auto-repair and troubleshooting abilities.
- FAQ or "support" tools to assist users in the event of a breakdown or anomaly.
- Strong physical characteristics to guard against adverse living conditions such as temperature, humidity, etc.

While there are not many public resources on IoT security best practices for end-users, some can help developers incorporate security best practices in designing IoT technology. One such example is the IoT Security Foundation's "IoT Security Compliance Framework". The segments of the compliance structure are related to the Hub-based architecture below.

Hub Functions	Compliance Framework Sections
Network Management	• Elements of the cloud and the network • Supply chain and manufacturing security
Connecting Devices Securely	• Interfaces for wired and wireless devices • Authorisation and authentication • Hardware encryption and key protection • Framework
Lifecycle Management	• Hardware and physical reliability of the system • Software for devices • The management context of the device • Transition in device ownership
Device Security	• Structures and accountability for business compliance • Web-based user experience • API for mobile devices • Confidentiality

Table 6: Compliance Framework Mapping

Focus 3: Industrial Control Systems

Overview of Industrial Control Systems

Industrial control system refers to a broad category of control systems that include DCS, SCADA, as well as other PLCs that are commonly used in industries and essential infrastructures. An ICS is made up of control components (i.e., electrical, hydraulic, mechanical, and pneumatic) that work collectively to build an industrial goal such as manufacturing, transportation, etc. The system's control section involves the requirement of the expected outcome or efficiency. Control may be completely automated or include a person in the process.

A large number of contemporary ICS are the result of the integration of IT functionality into established physical structures, frequently substituting or augmenting physical control mechanisms. In machines and motors, for instance, embedded digital controls have supplemented analogue mechanical systems. Savings and efficiency advancements have aided this progression, contributing to several contemporary "smart" innovations, including the smart power grid, industrial automation, smart homes, and advanced manufacturing. Although this facilitates the connectedness and robustness of these systems, this also increases the necessity for their versatility, sustainability, privacy, and security.

ICS Security Architecture

Ideally, it is suggested to distinguish the ICS network from the corporate network when designing a network architecture for an ICS development. Because the essence of network traffic differs between these two networks. If ICS network traffic is routed via the corporate network, it can be disrupted or exposed to Denial-of-Service (DoS) or Man-in-the-Middle attacks. Because its networks are distinct, scalability and reliability issues on the corporate network will unlikely influence the ICS network.

Practical issues, like the expenditure on ICS implementation or the maintenance of homogeneous network infrastructure, usually entail a connection between the ICS and corporate networks. This connection poses a major security concern and must be safeguarded with boundary detection systems. In this network section, servers holding ICS data that must be viewed from the corporate network are installed. Only these devices should be able to link to the corporate network. For any other interfacing, the firewall should only allow the bare minimum of approachability, which includes accessing only the ports needed for specific communication. These architectural considerations are outlined below:

Network Segmentation and Segregation

The purpose of network segmentation and segregation is to limit access to private data for certain systems and individuals while still allowing the enterprise to function efficiently. Typically, network segmentation and segregation are enforced at domain gateways. ICS environments frequently have many well-defined domains, like the operational LANs, control LANs, and operational DMZs, along with gateways to non-ICS and less reliable domains, like the Internet and corporate LANs.

Once network segmentation and segregation are executed properly, the amount of access to sensitive information is reduced. This could be established by the use of several mechanisms and practices. Some of the popular mechanisms and practices for offering good network segmentation and segregation, depending on the design and configuration of your network, includes the following:

- Encryption or network handset partitioning imposes logical network segregation. This could be accomplished using VLANs, VPNs that employ cryptographic mechanisms, unidirectional gateways, and other similar technologies.
- Incorporate techniques that go beyond the network layer. Where appropriate, each device and network must be segregated and separated from the data link layer to the application layer.
- Use the least right and need-to-know ideals. When a device does not need to interact with another device, it should be prohibited from doing so. A device only has to communicate with another device on a particular port.
- Differentiate information and infrastructure according to security needs. Along with network separation, virtualisation could be used to achieve the necessary segregation.
- Incorporate whitelisting rather than blacklisting; in other words, allow access to the identified good entities rather than refusing access to the identified threat.

Boundary Protection

Boundary protection systems are important aspects of architectural design that implement unique security procedures. Organizations may separate ICS and business system resources that carry out various missions or operations. Separating device components with boundary protection mechanisms allows for greater protection of individual components as well as more efficient monitoring of information flows among these components. Boundary protection devices decide if data transmission is allowed, often by inspecting the data or related metadata.

The placement of boundary protection devices is determined by the operational security architecture. The demilitarized zone (DMZ), a host or network segment incorporated as a "neutral zone" between security domains, is an effective design construct. It aims to implement the ICS domain's policy and procedures for the external exchange of information and to grant restricted access to external domains while securing the ICS domain from external risks.

Firewalls

Firewalls are systems or structures that regulate the flow of traffic between networks with varying levels of security. Firewalls will limit ICS inter-subnetwork interactions between functional security subnetworks and applications even further. An organization can prevent unauthorized access to the respective services and devices within the more critical areas by using firewalls to monitor connections in these areas.

Firewalls demand regular monitoring, preservation, and recovery. Rulesets must be checked to ensure that they are receiving proper defense in the face of constantly evolving cyber threats. System features should be analyzed to ensure that the firewall is collecting data and could be relied on in the event of a security breach. Real-time management of firewalls is needed to identify and respond to cyber incidents as quickly as possible.

Logically Separated Control Network

At the very least, the ICS network should be technically segregated from the corporate network. Implementing an intermediate DMZ network is a viable approach for facilitating connectivity between an ICS network and a corporate network. The DMZ should be linked to the firewall so that the corporate network and the DMZ, as well as the ICS network and the DMZ, can communicate. The corporate network and the ICS network must not communicate with one another directly. Implementing a Virtual Private Network (VPN) between the ICS and external networks will provide added security.

Recommended Defense-in-Depth Architecture

An ICS cannot be safeguarded by a single security product, infrastructure, or strategy. A multiple layer approach involving at least two (or more) separate overlapping security measures, also known as defense-in-depth, is desired to minimize the impact of any one process failing.

Figure 13 presents an ICS defense-in-depth architecture approach established by the NCCIC/ICS-CERT Recommended Practices committee and DHS Control Systems Security Program (CSSP). The document Control Systems Cyber Security: Defense in Depth Strategies guides designing defense-in-depth architecture techniques for enterprises that use control system networks while preserving a multi-tiered design concept.

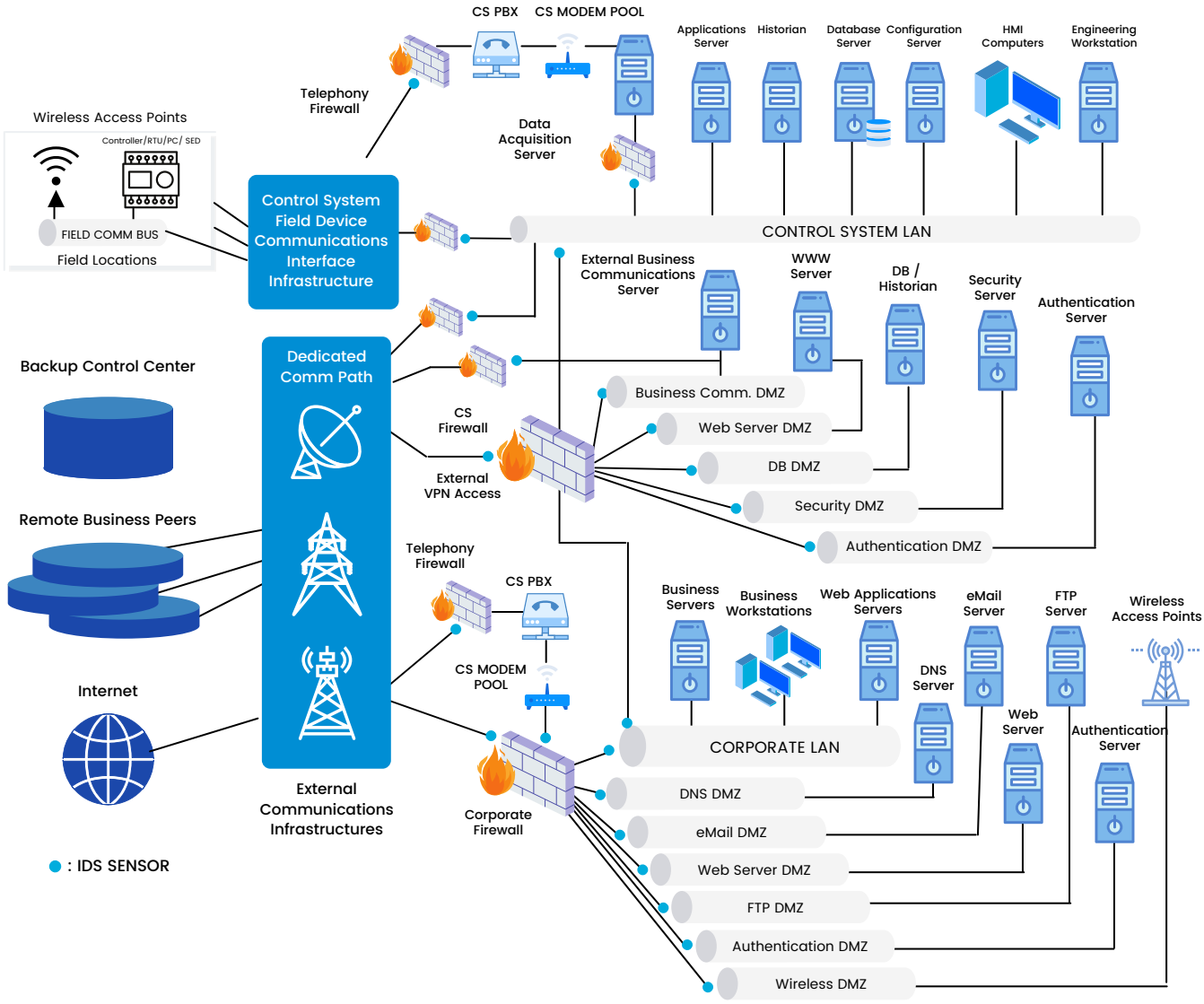


Figure 13. CSSP Recommended Defense-In-Depth Architecture

(Source: K. Stouffer, J. Falco, and K. Kent. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security. Sp800-82, NIST, September 2006.)

This ICS architecture includes firewalls, the use of demilitarized zones, and intrusion detection. The use of multiple demilitarized zones offers the potential to distinguish features and access privileges and has proven to be very efficient in securing huge architectures consisting of networks with varying operational mandates.

3.1 Overview of Cyberattacks in IoT

IoT has created entirely new businesses and revenue streams or delivers a more efficient experience for consumers. Along with this, it also creates new opportunities for all that information to be compromised. Not only is more data being shared through IoT among many more devices, but more sensitive data is being shared. As a result, the risks are exponentially greater. There are many classifications of IoT attacks. In this subsection, we have described the DDoS, Weak Authentication Attacks, Privacy Violations and Data Leakage Attacks, and Malware Injection Attacks. To an extent, we have further classified these attacks based on the IoT layers.

3.2 Distributed Denial of Service

Introduction

It is a DoS (Denial of Device) attack that uses multiple computers or machines to flood a targeted resource. It occurs when an attacker or attackers attempt to make it hard or impossible for a service to deliver by overloading it with requests to virtually anything: services, devices, networks applications and even specific transactions within the application. Since DDoS uses multiple systems, it will be hard to track the source system that is causing the attack, overloading volume is high, and due to the speed of this attack, it will be hard to detect flooding before it is too late, and the outcome/damage is high or sometimes even catastrophic. This attack can successfully affect compromised devices and systems. Some of the examples of DDoS attacks in IoT are Mirai –it is malware that infects smart devices that run on ARC (Argonaut RISC Core) processors, turning them into a network of remotely controlled bots or "zombies" This network of bots, called a botnet, inflects Linux systems, Reaper – Unlike MIRAI, REAPER majorly employs exploits that target disclosed vulnerabilities in IoT devices. Currently, many popular router brands as well as IP cameras and Network Attached Storage devices are affected.

How it Works

The control of the network and devices that help to execute a DDoS attack is necessary a step for the attacker shown in "Figure 14". Malware like bots or zombies software helps the hacker to gain control, then he sends commands to each bot remotely and then directs it to the desired source IP address. Therefore, if a hacker sends hundreds of commands to the equipped robots, there will be an overflow of requests in the target port or server. In this way, the service will be down for normal traffic.

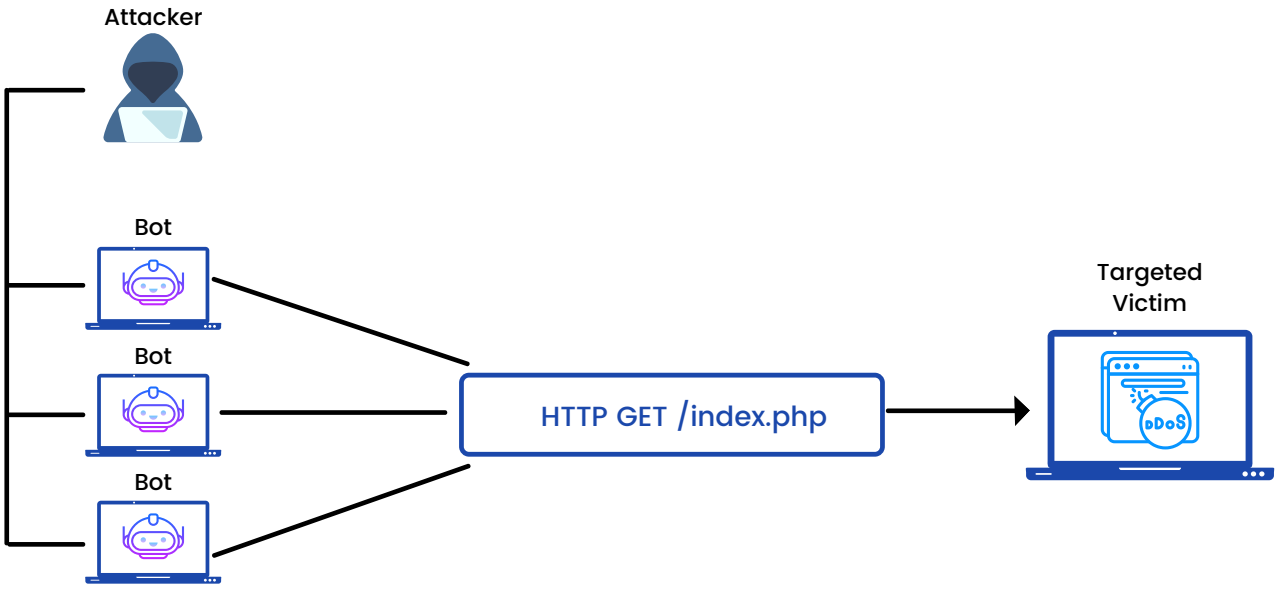


Figure 14: DDoS attack work

Classification of DDoS Attack on IoT

IoT is divided into three key layers that are Observation Layer, Network Layer, and Application Layer; in this subsection, we present DDoS attacks possible on each layer.

Types of Attacks at Different Levels:

1. Device Level

Attacks like Jamming - It prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on. The military uses jamming attacks as a tool to attack and disrupt terrorist's communications because the open nature of wireless networks makes them vulnerable to various attacks. This can occur when technique like RFID (radio-frequency identification) is used to receive and send the data from IoT sensors without any human interference.

2. Network Level

This layer is most vulnerable to attacks, as huge data is pumped through wired and wireless networks to carry out an attack. Examples of network layer attacks: ICMP (Internet Control Message Protocol) flood – happens when a hacker attempts to overwhelm a target device with ICMP echo-requests (pings). SYN flood attack (half-open attack) – occurs when the attacker aims to make a server unavailable to legitimate traffic by consuming all available server resources.

3. Application Level

Reprogramming attacks, Path-based DoS attacks are common in this layer. Mainly the application layer, which contains basic user interfaces like smart cities, smart devices, smart governments, etc.

Measures to Prevent an Attack:

1. Mitigating flooding

This defence is based on the technology of directing the harmful flood to an external server through a mediator, with a fee-based agreement for the mediator to protect IoT devices. This technique is used for attacks whose scale is very large.

2. Detecting intrusions

Network Traffic detection is considered one of the classical solutions to prevent DDoS attacks in the IoT networks, which goes toward the system-level model. To prevent the attack, it begins with capturing the attack, then defining the types of the hacker and finally applying the defence operation that is, the sabotaged device that sends larger than usually identified requests is disposed of, but we cannot prevent all the DDoS attacks with this technique. The prohibition technique is considered a modern method that works successfully for IoT devices. It has software whose mission is defencing (SDN – Software-defined networking) its primary objective is to effectively detect and mitigate the attack using software features, i.e., it monitors all the data transmission received by IoT devices and sends an alter to mitigate the exploits when a suspicious interaction is detected.

3. Blockchain defence

The blockchain mechanism is another modern defence method to protect IoT devices. As organized records are kept in the blockchain, the IoT device is connected to servers in a sequence. Launched applications for IoT devices are built into this blockchain, with the status logged each time an interaction occurs between the server and IoT device. When IoT devices are major buildings and cities, it would be better to monitor them and protect them using blockchain.

3.3 Hardware Security

Overview

The term hardware security refers to utilizing physical devices to protect our IoT devices. Hardware-based security solutions boost the device's performance and work more efficiently. These solutions are operated on a chip, and they are enhanced well to perform their tasks. They follow two procedures encryption and decryption, and it is far more efficient than any other normal processor. Sensitive data such as keys and random generators are encrypted into the hardware, which in turn will be difficult to trace.

Implementing a hardware solution may be costly, and sometimes it requires a lot of time and effort, but this can help to keep our sensitive data safe and assures that it does not get leaked. Hardware security has been in more demand along with SoCs, microprocessors, and microcontrollers. These devices can be used to check the flow of the network traffic. Hardware security can be added as an extra layer to secure the systems. It is very important to access and pay attention to the vulnerabilities which are present while manufacturing as well as to the potential codes and the data on the network.

Types of Attacks on Hardware

Several types of security attacks can be planned on hardware. Here is the list of the attacks:

Side-Channel Attack

It is a kind of attack in which a secure system is attacked using an insecure system, i.e., the system that is not secured. For example, the attackers can easily access the file if they remove the hard drive and connect it to another pc. This is used to check parametric behaviours, i.e., Power, Timing, and EM, to pull out the hidden data. There are some other examples and these attacks in which we can get the data that resides in the chip by managing and analyzing the channels, i.e., physical signals.

The information embedded in the side-channel parameters will depend on the computation of the intermediate values while executing the crypto-algorithm and comparing it with the inputs and secret key of the cypher. An adversary can efficiently extract this key by observation, and he or she can achieve it with the help of a low-cost tool in a minimal amount of time, ranging from few minutes to few hours.

Rowhammer Attack

In this attack, the values which are in the row of a memory cell are modified and thus result in alteration of the neighbour rows. They can insert malicious codes that may consist of kernel-level privileges. It represents a bit flip in the DRAM memory that can result in privilege escalation or other malicious things. These types of errors can occur in the memory because of the background radiations and neutrons.

Bit errors that can be controlled up to some limit and are repeatable can cause a major threat to security. An attacker uses the targeted bit flip to a certain memory location that gives the read permission for the restricted memory.

Hardware Trojan Attack

It is a kind of malicious circuit that destroys the function or reliability of the electronic system. The Trojan functions consist of removing, controlling, altering, and sneaking the design contents. It is difficult to find the stealthy Hardware Trojan. The SoCs that are spoiled can see a difference in their working. Sensitive data may be leaked, or it may suffer from poor performance.

There is no device implemented to detect these Trojans. We are unaware of its size, type, and location. Activation happens very rarely. A Trojan is well hidden during the normal working of a chip, and it is activated only when triggering conditions are applied.

Physical Attack

Modern PCBs typically integrate with ICs with high pin complexity and a huge number of components with a miniature layout. Current PCBs operate at 1-10 GHz to support high-speed data communication. Since they are more complex and have so many layers in them, System Integrators rely on third-party designers. Counterfeiting has become a major issue in the PCB industry. Its features can help in making countermeasures, i.e., the JTAG infrastructure can be used for trust validation.

Research on PCB products shows that PCBs are designed in various countries. If we rely on a third party, the PCB can be untrustworthy and have a greater degree of vulnerability. Today's PCB designs consist of 20 to 30 layers and embedded passive components to minimize the form factor. This will allow an attacker to tamper with the internal layers to modify the design or change the components.

Reverse Engineering

This is also known as backward engineering, and it is the process in which one tries with very little insight to know how a device, process, system, or piece of software manages to finish a task. This technique does not only deal with just making a duplicate or modifying an artefact. It is just an analysis to reduce design features with some amount or not much knowledge about the steps to build the system all the way to the actual production.

The main aim is the redocumentation of legacy systems. If a competitor uses a reverse-engineering method, the goal is not to copy it in toto. It is to perform a competitive analysis. It is used to interface one system with another system. Knowing about the enemy's research by taking their data and dismantling it could yield insights to produce the same product or result in a good countermeasure.

Hardware IP Piracy

Hardware IP means portable hardware intellectual property. It is a renewable and computable unit of the logic cell or IC layout generally designed by an IP vendor. These are different hardware IPs: Soft IP, Firm IP, and Hard IP. The issue of security comes because these will be supplied by different vendors from all over the world.
Some rogue people in the foundry illegally copy the IP and distribute it to unauthorized persons. An attacker can steal it and take the design ownership. We should thoroughly check the details of IP vendors. Security in OS should be enhanced. Persistent encryption should be done to maintain system security.

Mod-chip Attack

This type of attack is generally carried out by connecting wires to particular points on a system circuit board. These Mod-chips alter the system h/w and s/w protection. These chips consist of one or more integrated circuits joined with distinct points on small PCBs. These are known as drive chips that affect the running of the system by overriding security. These chips consist of a microcontroller, FPGA, or CPCD to attack the system.
This could be prevented by removing attack points that are used by the mod-chip by doing modifications to the PCB arrangement. LPC bus is used at the time of testing the system. Keeping it secure by additional tamper detection and protective circuit on a PCB.

Security Architecture Attacks

Simple mistakes in IC design can expose the IC to a lot of attacks. Vulnerabilities will be introduced in ICs in the form of some changes such as Hardware Trojans, backdoors, etc. Even now, many tools are not fortified with security measures. Due to the increase in manufacturing ICs, the design houses depend on third parties with no proper verification.
It is crucial to find weaknesses during hardware design and validation. It is nearly impossible to fix design and architecture problems past this phase. Detecting and fixing it at a later stage is extremely difficult and involves a much higher cost.

Examples of Hardware Security

Crypto Acceleration

This is one of the primary forms of hardware security and secondary to hardware defence. It is a technique that uses cryptographic functions that not only speed up the applications but also provide hardware with systems that cannot be exploited in software. For example, a software-based AES may cause a code injection attack, but it is difficult to attack hardware-based AES.

True Random Number Generators

Random Number Generators are generally written in software and have therefore made the job of the attacker very simple. Let us consider a scenario in which two security experts are controlling the jeep from a remote place. This is done by connecting to the car's multimedia system, and they send their messages through the CAN bus. Hence this can result in the attacker taking full control of breaks, accelerator, and steering.

Memory Encryption

Earlier, memory-related processes directly moved the data which was stored in memory (RAM and ROM). This had the vulnerability that the unencrypted data could be stolen. But now, there are encryption options, which ensure that even if the attacker reads the contents of RAM or ROM, without the exact hardware, he or she cannot use the data.

Secure Boot

Designers have introduced a method called secure boot in the processor where it begins by running the boot code, which cannot be modified and is thus immune to code injection attacks. After this, it checks the application which is about to be loaded as well as the code integrity. In case the code is injected, the system will run only up to some stage, or it will show the warning that the code injection has been found in the system.

Trust Zone

Trust zones can help to deal with the situation if the user is not aware of whether the code that he or she runs is malicious. There may be some CPU instructions that can be dangerous, and they can access hardware, pointers, and critical systems. Therefore, modern processors have certain advantages in which the OS operates on the highest privilege and can access all the instructions, whereas, the processes that the OS executes are put on the lower privilege. These processes cannot use sensitive data, and hence they are less prone to attack a critical system or a processor.

Tamper Pins

Tamper pins are one of the most useful hardware features because they are difficult to detect and prevent. Sometimes attackers have to physically remove the parts to use the I/O, such as debugging the ports and memory. These pins can trace out the mechanical event that has occurred, such as the opening of an enclosure. Once it is found out, it can instruct the processors to do a specific task which consists of a simple reboot to protect sensitive data being read. It is also used to obscure the pins which are not visible to the attackers.

3.4 Hardware Security v/s Hardware Trust

Hardware security issues come from vulnerabilities (i.e., Side-Channel Attacks or Trojan attacks) at different levels and due to the lack of robust security for software and system. Similarly, hardware trust issues appear from the untrusted entities of the hardware life cycle which includes untrusted IP or CAD (Computer-Aided Design) tool vendors, fabrication, test, or distribution facilities. Such parties misuse the hardware components or system.

The table below represents some of the major concerns that occur due to untrusted design, fabrication, and test processes for an IC. The same can be considered for an SoC life cycle that integrates the IPs typically acquired from third-party vendors into a design that meets functional and performance criteria.

IC Lifecycle	Attack Vectors	Counter measures
IP-Vendor	A Hardware Trojan acts as a hidden front door inserted in the chip by using an ASIC semiconductor that we can get from a non-reputable source, or it can be inserted by a rogue employer.	Verified Hardware IP Trust
SoC Design House	Some well-known IP piracy threats such as reverse engineering and malicious circuit modifications are a major concern.	Hardware obfuscation can help to prevent piracy as well as Hardware Trojan attacks.
Foundry	The foundry strategies are designed based on each stage of the Technology Life Cycle (TLC).	We can apply the techniques such as physical inspection and advanced image processing.
Deployment	• Side-Channel Attacks • Reverse Engineering • IP Counterfeiting	• Side-Channel resistant design • Hardware obfuscation • Hardware Authentication

Table 7. Attack Vectors During an IC Lifecycle

3.5 Embedded System Hardware

An Embedded System is a microprocessor- or microcontroller-based system made for a specific use and surrounded by a giant mechanical or electrical system. Since these are made for some specific tasks instead of a general-purpose system, their size, power, and cost are limited. These are applied in commercial, military, and industrial applications. Some embedded systems may have Real-time Operating Systems (RTOS), whereas some do not.
Generally, hardware-based embedded systems are used to calculate real-time operations. As a microprocessor is just a CPU, other components of the system should also be integrated.

Characteristics of an Embedded System

- Task-specific: An embedded system is made for a specific use/task, for e.g., a fire alarm is an embedded system which senses smoke.
- Tightly constrained: The embedded system is tightly resourced and time-constrained. For e.g., an embedded system must be quick and task-tolerant, with limited memory and minimal power consumption.
- Real-time and reactive: Real-time or near real-time is required in many environments. For e.g., a GPS should provide road and location data and must alert users to increase situational awareness in a real-time or near real-time manner. Any delay can cause catastrophic results.
- Hardware/Software Co-design: The hardware part is used for performance and security, and the software part is used for flexibility and features.
- Microprocessor/Microcontroller based: These are designed at the heart of the embedded system and used to perform operations.
- Memory: Having a memory is essential as programs are loaded are stored into the memory.
- Connected Peripherals: Peripherals are used to connect input and output devices.

Embedded System Security

Embedded system security is one of the traditional methodologies to keep our systems secure by preventing threats. These are designed to perform some specific tasks. We can get these systems in process control systems, aircraft, and other applications. Because of their minimal size and limited resources, designers and developers may face some security issues.
Firmware in the system is almost impossible to update, and therefore in the past, some systems were designed to have a lifecycle of at least 15 years. With the IoT, the nature of embedded systems is changing, and the attack vectors are also growing exponentially. An embedded system attached to the smart device can be hacked to control small thermostats to industrial control systems.
We have to take embedded system security as an end-to-end approach during the design phase, like taking security in the IT field. These security issues should include the cost of an attack and the number of possible attack vectors.

The solutions to these embedded attacks are:

- Regularly updating the firmware.
- Using the firmware according to the need-to-use basis.
- Monitoring the networking connections to and from embedded systems.
- Integrating with third-party management systems.

Properties of Securing an Embedded System

To attack an embedded system, it requires only a single vulnerability to create an exploit. Therefore, if the defender wants to secure his or her system, he or she must think thoroughly and be well prepared to get protected from any possible vulnerability. Any opening can make the attacker's work simpler. They can steal your information, control your data, and create exploits for others to use anytime and anywhere.
It is also possible for an attacker to use an initial compromised device to pivot from one subsystem to another that may cause further damage to our networks, tasks, and reputations.
To achieve security, here is the list of 10 properties of highly secured embedded systems based on experience in engineering security solutions from various platforms. These properties will assure that it will make the attackers' work difficult.

Design Principle	Description	Implementation
Data-at-rest protection	Software, data, and configuration files will be safe if kept in non-volatile memory, especially when using encryption.	• Full-disk encryption • File encryption • TPM/HSM
Authenticated/ Secure Boot	It will be authenticated and/or decrypted before using that software (including firmware and configuration data). It will be authenticated and/or decrypted.	• TXT, Bootguard • UEFI SecureBoot • Application Whitelisting
Hardware Resource Partitioning	Hardware resources are segregated such that they can perform functions individually up to the maximum possible degree.	• MMU/Paging • Multi-Core/Multi-Socket • Cache Allocation Technology

Design Principle	Description	Implementation
Software Containerization and Isolation	Software should be well-defined, self-contained, and isolated.	• Process Address Spaces/Virtual Memory • Dockers/Containers • Virtualization/Hypervisor
Attack Surface Reduction	• Minimize Dependencies/Trusted Computing Base • Minimize Codebase • Limited and well-defined interfaces	• Code removal • Network and Application Firewalls • Software Guard Extensions (SGE)
Least privilege and mandatory access control	Users and applications can get only limited privileges by using non-bypassable Memory Access Control (MAC).	• SELinux/AppArmor/SMACK • SECCOMP/chroot • XSM/FLASK (hypervisor)
Implicit Distrust and Secure Communication	Communication with external sources is only allowed after authentication.	• SSL/TLS • Identity and certificate management
Data Input Validation	Information received from untrusted sources should be validated before using them in our software applications.	• Data Format Filters • Cross-Domain Guards
Secure Software Development, Build options and OS configurations	Software applications and OS Kernel shall be compiled and configured with the available security options enabled.	• Type and memory-safe languages • Build Parameters • Kernel Configuration
Integrity monitoring and auditing	Systems monitor the integrity and logging the audits of security-related events.	Continuous Memory Hash Verification

Table 8. Properties of Highly Secured Embedded Systems

Data-at-rest Protection

In this type, the data is stored on a device either encrypted or follows definite protocols, including encryption to secure our data from unauthorized access. The storage components consist of hard drives, flash memory, and USB thumb drives. Many recent embedded systems have encrypted-storage protection requirements determined by intellectual property protection, digital rights management, sensitive customer data, and more.

The flowchart below represents the different layers in which we can protect our data which is at rest.

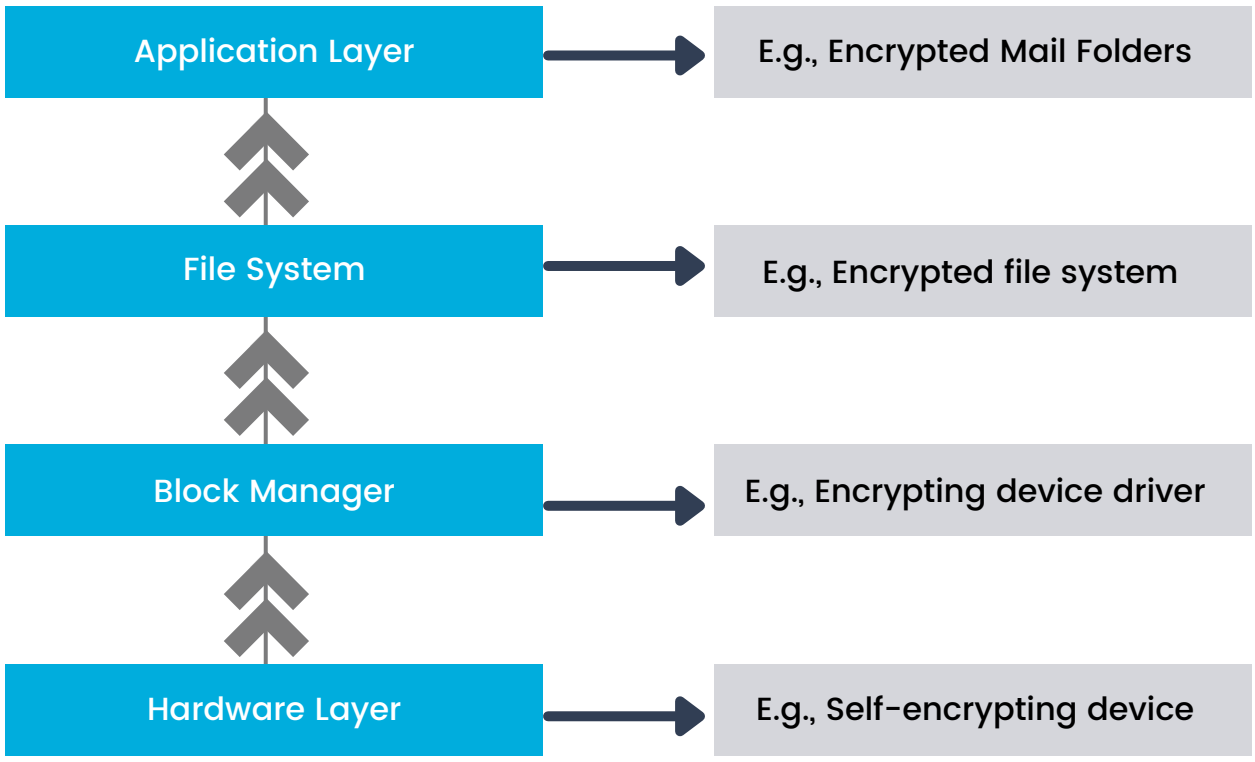


Figure 15. Flowchart: Different Layers in Data-at-rest Protection

3.6 Data Layers

Hardware Layer

The whole medium used for storage is encrypted by using FDE (Full-Disk Encryption). It encrypts all the information, including hidden files such as OS temporary files and swap space. The benefit is that the file cannot leak. But if the drive is unencrypted, it can expose the boot records.
We manage our FDEs within the medium peripheral called SED (Self-Encrypting Device). Nowadays, these devices are common in every laptop shop. The advantage is that no new or minimal software is written to make use of the data-protection facilities. If self-encrypting storage media is possible, it is the best alternative because of its easy use and excellent performance, and it can hide the storage encryption key from the main application and memory.

Block Manager Layer

We can carry out the encryption at a higher level, the device-management layer, typically a block-oriented driver. Such a kind of protection can cover the overall managed device (FDE). However, the execution may vary. If it consists of an encryption accelerator that is symmetric, there is a chance of overhead. Perhaps, implementing pure crypto-software can cause a severe loss in performance.

File System Layer

The major use of this layer is to provide well grossness over the choice of information that needs storage privacy. This is very much important if the encryption is performed in software with minimal or no hardware acceleration. Based on the implementation of the file system, developers can decide whether they want to encrypt at the volume level or the individual file level.

Application Layer

After doing all the above steps, at last, applications can add their data protection by using underlying file-system encryption features or a custom implementation. E.g., an audit logging device can encrypt its audit records before calling the standard file system output functions. For volume, file, or application-level data protection, developers can make separate keys for these groups of data instead of a single key for the entire system.

Authenticated/Secure Boot

Secure Boot is when OS boot images and validates code against the hardware before being used in the boot process. The hardware is already made to authenticate only the codes according to the security credentials that we trust. In simple words, it makes sure that the version of the OS and the boot software are from the intended manufacturer and have not been tampered with by malicious or malware third parties.
It can be used for a single device, e.g., i.MX6 processor is specifically used for e-reading. At Boot, the locked-down Linux is a good choice to consider. Once we design our boot images on this processor, we have to generate a secure key against an SSL certificate. For more integrated systems such as IP cameras operating on Linux, it is advisory to use Secure Boot because malicious boot code can lead to circumstances where the device is a part of a botnet.

Use the following methods to Secure Boot on i.MX6:

- Secure Process
  If we want to go down the route of Secure Boot, the surrounding processes should be well prepared and secure. Keys leaking out of the production environment can result in exfiltration.
- Strong Encryption
  The encryption should be very strong. It is very easy to generate weak keys and is a common problem. The algorithms should be up to date.
- Code Checking
  The remaining code in the bootloader, OS, and other software should be well written for Secure Boot, and make sure it lacks security holes to make Secure Boot meaningful.
- Authenticate Anywhere
  For proper security, we have to authenticate the code as much as we can and make sure that it follows the practices made for the libraries. Securing the process depends on how the keys are generated and stored.
- Proper Authentication
  It is very important to ensure that the code is genuinely performing the secure Boot. We can even move from a secure piece of code to an arbitrary location in memory to continue with the execution. It is essential to ensure that the code authenticates the next step of the code to maintain its security.

Hardware Resource Partitioning

Hardware partitioning divides resources into many server entities where OS and applications work independently. This is more useful since application-related hardware is much faster than software. But this hardware is very costly. Software is cheaper, but it works slowly. Therefore performance-critical components should be realized in hardware and non-critical in software. In this way, we can achieve a good trade-off between cost and performance.

Hardware and software designs are inadequate for some specific tasks. Composing hardware and software can create problems. E.g., communication and system architecture-related issues. Hardware-Software Co-Design (HSCD) methods can be used to overcome this problem. Partitioning is the necessary step while designing HSCD, i.e., which components should be used for realizing the hardware and which components for software. The above-defined step can help in finding the optimal trade-off between cost and performance.
Generally, partitioning is done manually. Since the system design is becoming more and more complex, this method turned out as infeasible, and researchers are trying to automate the partitioning as much as possible.

Software Containerization and Isolation

Containerization has become popular in the development of software as an alternative or companion to virtualization. It involves the packaging of codes and their dependencies to run in a uniform and consistent manner.
The technology is upgraded every day, giving developers, operations teams, and software infrastructure an advantage. This technique enables them to produce and deploy applications more securely. By using special methods, code is made in a specific environment. When this is sent to a new location, bugs and errors may occur.
Containerization can remove this problem by bundling the application codes with related configuration files, libraries, and dependencies required to run. This single package is far away from the host OS. Therefore, it stands alone and becomes moveable.

As regards isolation, many embedded systems include on-chip FPGA (Field-Programmable Gate Array) along with processors to meet the high computation demand to provide flexibility to users to add custom hardware accelerators. We can capture sensitive data by using these accelerators or with the help of hardware Intellectual Properties (IPs). The built-in accelerators in embedded systems cannot help in preventing unnecessary access to the IPs causing a harmful security breach. There is an approach used called FPGA accelerated embedded system design. This inherits MAC-based authentication policies operating at software, bringing it down to hardware accelerators in FPGA. It ensures proper use of confidential data to prevent software-originated attacks at hardware IPs and data leaks.

Attack Surface Reduction

Commonly there are 12 attacks, and each of these attacks is divided into three subcategories depending on their targets:

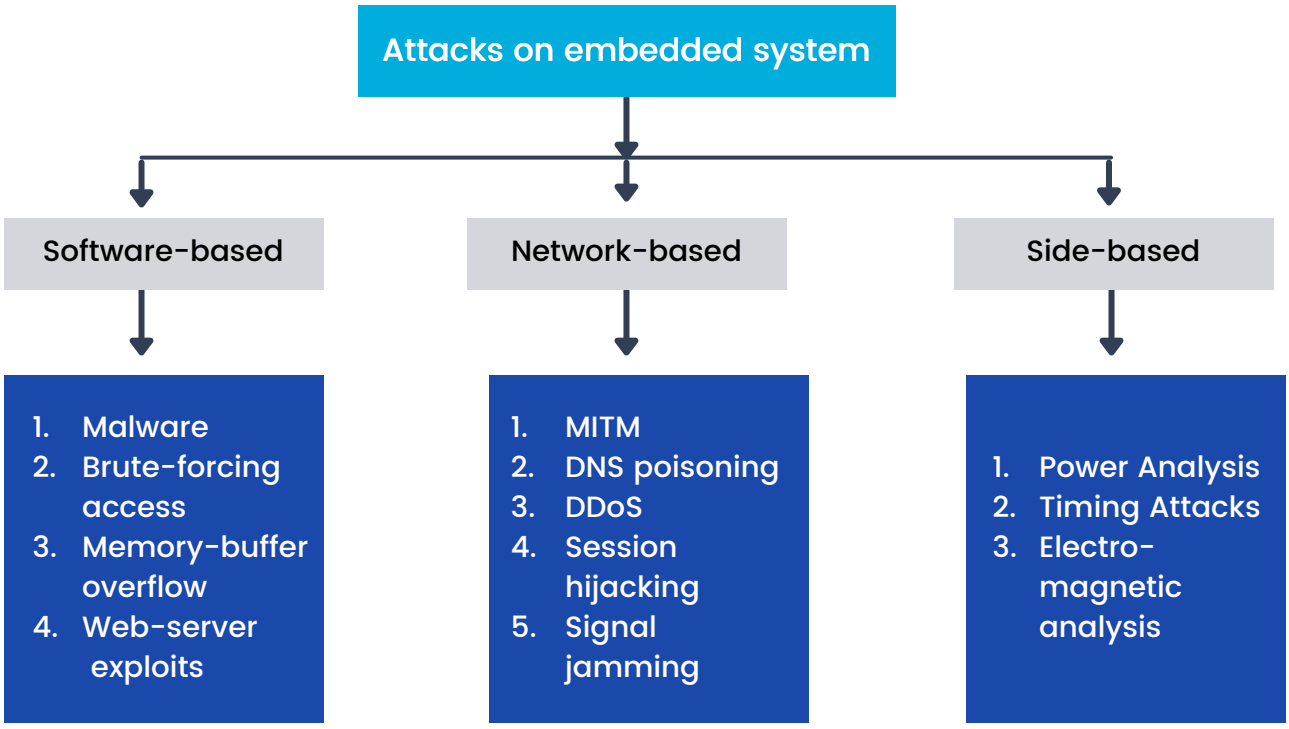


Figure 16. Categories of Attacks on Embedded Systems

Best practices are defined to reduce these attacks. Developers need to be thorough with the industry standards for embedded software development and learn effective measures and practices before coding. The below figure defines 11 best practices, and each is divided into subparts that can make our protection even more reliable at all development stages, from design to support.

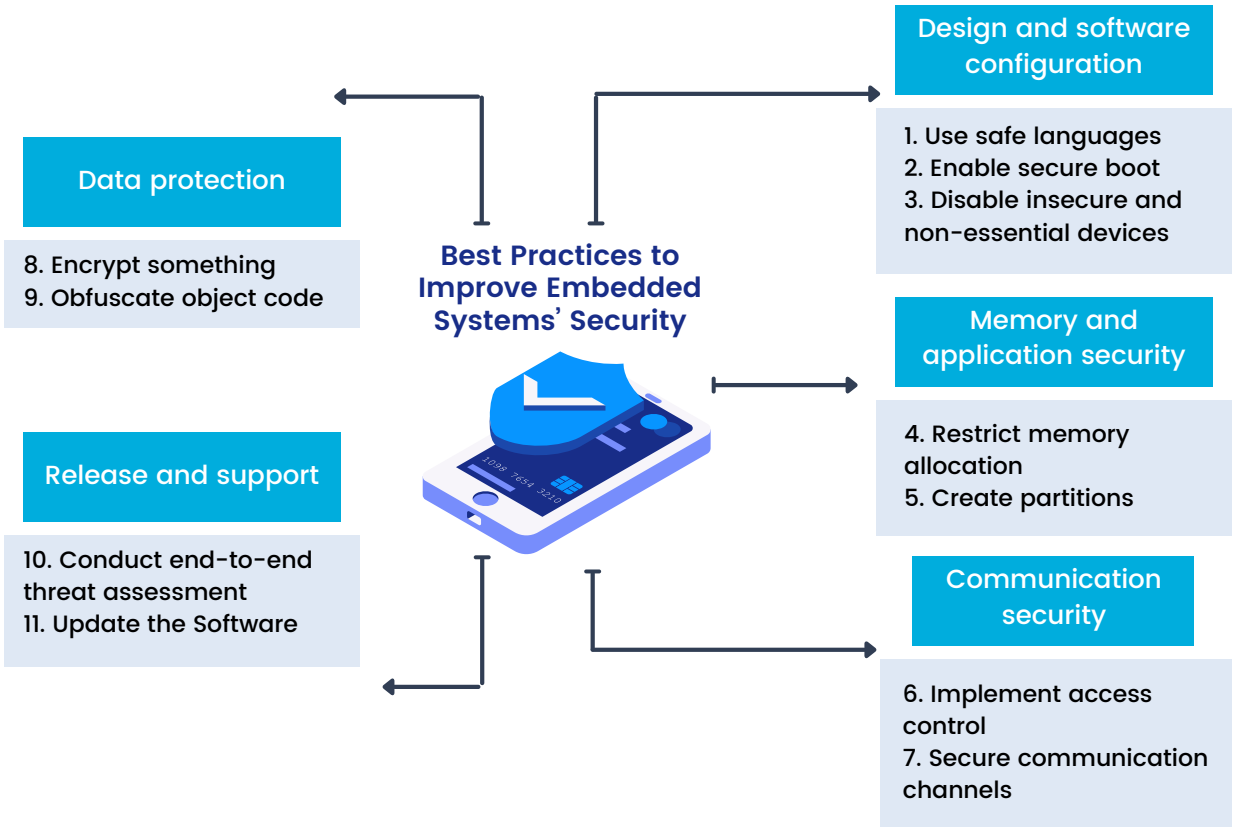


Figure 17. Best Practices to Enhance Embedded System Protection

Least Privilege and Mandatory Access Control

The least privilege concept says that only small privileges should permit systems software components to do their essential tasks. Applications only can use the minimum set of interfaces and services required to do their work. Most software developers and system engineers use the shortest method, i.e., explicitly granting excessive privileges to applications with the supposition of a trusted operator or activities of an application, a practice that an attacker can easily compromise.
Therefore, the embedded systems should be made with Mandatory Access Control (MAC). MAC checks for access grants and restriction policies at the time of system design. These controls are always imposed on the fielded device. Within the fielded device, it is impossible to bypass the security controls.
Even if attackers succeed in compromising systems sub-component or gain root-level access, they cannot change or disable security settings. Using both techniques frustrates the attackers and blocks their ability to modify, disable, or interrupt system services.

Implicit Distrust and Secure Communication

Let us consider a scenario where a person receives a call from an unknown number and is asked to share their credit card number. The obvious answer would be a "No". In the same way, communication from external sources to our system should be denied until the remote source has been authenticated. The simple way to say it is that a security system does not permit any other systems to talk. It compels the external systems to prove who they are. The starting point for a secure communication system should be default-deny.
Coming back to the scenario, the way we give credit card information only to a person we trust, that too in a closed room where no one hears, our system should also enforce secure communication despite having authenticated other parties.
These properties can be deployed by using protocols such as SSL and TLS with identity and certificate management. When crypto comes into the picture, there is always a question on how to secure these TLS keys and certificates? Using mutual authentication and encryption, without a doubt, we can state that the communication is happening only between the trusted entities (not the attacker), and no one can listen to our communication.

Data Input Validation

Most of the developers could not figure out how attackers inject malicious inputs causing the software to get damaged. Giving data into the system via any crossing point can exploit software vulnerabilities to get restricted access or corrupt system application memory to create a denial of service. A secure software design cannot perform any guess on the acceptability of the provided data and performs validation of the format and the contents written in it before being processed by the rest of the system.

There is a requirement for an additional examination of the input given by the user. Each device should check the agreement of the messages to a predefined data standard as they are passed from device to device.
Secure software architecture always follows the principle of mutual distrust. Components residing in the system have to prove themselves well through a continuous authentication step. Moreover, authentication expires for a given period and should be renewed.

Secure Software Development, Build Options and OS Configurations

Some options are given to notify us of many types of potential security and to get security enhancements such as:

- Detecting signed/unsigned conventions.
- Warnings for using format functions that can show possible security issues.
- Making use of 64-bit random address randomization.
- Compilation of code with unintended return addresses.
- Lightening various spectres.
- Defeating stack smash attacks.
- Preventing stack and heap against code execution.

If we are able to specify our programming language, we can remove all classes of software vulnerability in the code. Properly following the code practices, secure build options, and modifying the end system to maximize the security, there is less chance for the possible attacks to compromise most parts of the system.

Integrity Monitoring and Auditing

Finally, it is impossible to determine an attacker if we do not know when our system has been targeted. Here integrity monitoring and auditing play a major role. These are essential methods to find out when the device has been attacked or has been compromised. These alerts can help us to stop the attackers before the situation becomes worse. Some techniques include network and OS-level anomaly detection, system log monitoring, and scanning for known malware. This allows system operators to take action against attackers.
Auditing is a must for many compliance regulations as they support organizations to check for unauthorized tampering of necessary files, data, or other aspects of a system. Well-implemented auditing and monitoring allow us to know when we are attacked, fix the damage, and enable us to recover quickly, preventing loss of time, revenue, and damage to reputation.

Privacy Violation and Data Leakage Attacks

Mishandling a user's password, social security numbers, and other private information can compromise user privacy and is often illegal. Privacy violations occur when private user information enters the application, and the data is written to an external location such as the console, file system, or network. Physical or electronic data leakage is the unauthorized transmission of data within an organization to an external recipient. Examples of such attacks are Cross-Site Scripting (XSS, refer to the subsection on page 58), Eavesdropping, Phishing attacks, Node capture (tampering), Wormhole attack, Backdoors, and exploits. The following table will describe the attacks in each of the three layers in an IoT device with its countermeasures.

Layer	Attack	Counter measures
Physical Layer	Eavesdropping	Link-layer encryption, key-pre-distribution
	Node capture	Tamper resistance hardware, disabling JTAG and/or protecting bootstrap loader, camouflaging
Network Layer	Wormhole	Location-based keys, centralized computing
Application Layer	XSS	Filter input on what is expected upon data arrival
	Backdoors and exploits	Intrusion Detection System
	Phishing	Rotate passwords regularly and do not give information to an unsecured site

Table 9. Data leakage and privacy violation attacks table

Weak Authentication Attacks

Authentication can be viewed as the first line of security by enforcement of security measures at level 0. Weak Authentication describes any scenario in which the strength of the authentication mechanism is relatively weak compared to the value of the assets being protected and scenarios in which the authentication mechanism is flawed or vulnerable. When the control system of the IoT has a weak authentication system, the attacker can log in by brute-forcing or using the default password lists. This subsection describes and classifies different IoT attacks occurring at the Application level, Network level, and Device-level as shown in Table 10.

	Threats	Attacks	
		In transit	At rest
Device Level	Limited resources; Architecture; Interface; Software	Firmware; Brute force; Defraud; DoS;	Firmware; Physical; Credential.
Network Level	Architecture; Openness; Protocols.	Eavesdropping; Device scan; Spoofing; Man-in-the middle Reply; Unknown Key sharing	Device Scan; Brute force
Application Level	Interactions; Constraints; Environment; Human.	Impersonation; Malware; Insider.	

Table 10. Classification of Authentication threats and attacks

Firmware Hijacking

If firmware updates downloaded by an IoT device are not checked to make sure they originate from a legitimate source, an attacker can hijack the device and download malicious software.

Device Scan Attack

Adversaries scan devices in HIS to gather network information of these devices before launching sophisticated attacks to undermine security systems. Commonly used scanning techniques to gather computer network information include IP address scanning, port scanning, and version scanning.

Man-in-the-middle Attack

The attacker over the internet intercepts the communication between the two nodes. They obtain sensitive information by eavesdropping.

Identity Spoofing Attack

These attacks are easy to launch in an IoT access network. By using a faked identity such as the MAC (Media Access Control) or IP (Internet Protocol) address of the legitimate user, an attacker can claim to be another legitimate IoT device. The attacker can then gain illegal access to the IoT network and launch more advanced attacks, such as man-in-the-middle attacks and denial-of-service attacks.

Malware Injection Attacks

In an injection attack, an attacker supplies untrusted or malicious input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program. As injection attacks are a very well-understood vulnerability class, many freely available and reliable tools allow even inexperienced attackers to abuse these vulnerabilities automatically. Malware injection attack is a sub-category of Injection attacks. Here the cyber attacker creates a malicious application and injects it into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), respectively. Once the injection is completed, the malicious module is executed as a normal code in the cloud infrastructure. Now the hacker can launch any sorts of attacks such as eavesdropping, data manipulation, and data theft. The two common forms of this attack in cloud computing platforms are the Structured Query Language (SQL) injection attack and the cross-site scripting attack.

SQL injection attacks

Server-side vulnerability attacks target SQL servers in the cloud infrastructure that run vulnerable database applications. Thus, the vulnerabilities of the web servers are exploited, and then the hacker can inject malicious code in order to avoid the login credentials and gain unauthorized access to the backend databases. If this attack is successful, then the attacker can even change the contents, retrieve confidential information, remotely execute the commands, or even take control of the webserver for further criminal activities. These attacks can also be launched by a botnet. For example, the Asprox botnet used a thousand bots that were equipped with SQL injection kits to fire an attack that affected 153,000 different websites that were hosted on various cloud infrastructures.

Cross-Site Scripting (XSS)

It is a client-side vulnerability where an attacker injects malicious scripts such as JavaScript, VBScript, ActiveX, HTML, and Flash into a vulnerable dynamic webpage in order to execute these scripts on the victim's web browser. Later, the hacker could steal the user's cookies information used for authorization for accessing the user's account or tricking him into clicking a malicious link. For example, cyber researchers in Germany have successfully accessed all the customer's data in an AWS session using this XSS attack.

Measures

- The first step in preventing a SQL injection attack is by knowing the vulnerable applications by either self-imposing the attacks or by using penetration tools available online, which help the user to identify the vulnerabilities present in an application.

- Some of the steps to prevent the attack are -
  1. Validate user inputs by establishing a whitelist of all valid SQL statements and leaving unvalidated statements out of the query.
  2. Sanitize the data by limiting the special characters to not allow string concatenation.
  3. For writing all database queries use prepared statements with parameterized queries (variable binding)

     By following the above steps, users can differentiate between user input and code, actively manage patches and updates, limit read access and perform regular auditing and penetration testing.

- XSS attack can be prevented by the following mechanisms:
  1. **Filter input on arrival:** Wherever user input is received, filter strictly based on what is expected as valid input.
  2. **Encode data on output:** In HTTP responses where user-controllable data is output, encode the output to prevent it from being interpreted as active content. Depending on the output context, it might require applying combinations of HTML, URL, JavaScript, and CSS encoding
  3. **Use appropriate response headers:** Content-Type and X-Content-Type-Options headers can be used to ensure that browsers interpret the responses in the way you intend. This helps prevent XSS in HTTP responses that are not intended to contain any HTML or JavaScript.
  4. **Content Security Policy:** You can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities.

4.1 SCADA System

What is SCADA?

SCADA stands for supervisory control and data acquisition, and it is a software and hardware system that offers production facilities to:

- Manage manufacturing processes on a local or remote level.
- Data collected is monitored, acquired, and analyzed.
- Human-machine interface (HMI) software allows you to communicate directly with equipment including sensors, valves, pumps, motors, and more.
- Create a data source file to keep track of events.

SCADA is a set of computing devices (both software and hardware) that work together to control a system. Statistical data from factory floor devices such as pumps, valves, and transmitters are the starting point for this component collection.
The information gathered from the field devices is subsequently sent to a processor, such as a PLC. The information is distributed from the CPU to a network device system.
HMIs, end-user PCs, and servers are examples of these devices. Visualization of operator activities, such as controlling pumps and adjusting valves, are available on the HMI and end-user computer. This information can also be examined and used to improve plant productivity and solve problems.

Main components of SCADA:

1. Supervisory computers: These are the backbone of the SCADA system, collecting data on the process and sending commands to field equipment. It contains the HMI software running on operator workstations, as well as the computer and software responsible for connecting with the field connection controllers, which are RTUs and PLCs.

2. In compact SCADA systems, the supervisory computer could be a standalone PC, and the HMI may be a part of that computer. The master station in larger SCADA systems may have several HMIs housed on client computers, multiple data acquisition servers, distributed computer programs, and disaster recovery facilities.

3. Remote terminal units (RTUs): link to process sensors and actuators and are networked to the supervisory computer system. RTUs feature embedded control capabilities and frequently follow the IEC 61131-3 programming criteria. They can be programmed using ladder logic, a data flow diagram, or several different languages.

4. PLCs: or programmable logic controllers, are coupled to sensors and actuators in the process and networked to the supervisory system. PLCs often have a high-speed link to the SCADA system in factory automation.

5. PLCs may connect directly to SCADA over a wireless link in remote applications, such as a major water treatment facility, or they may use an RTU for communications management. Instead of using an RTU alone, PLCs are frequently utilized for remote sites with a significant I/O count for cost considerations.

6. The communication infrastructure connects the supervisory computer system to the RTUs and PLCs, and it might employ best practices or manufacturer-specific protocols. Both RTUs and PLCs regulate the process autonomously in near-real-time, using the most recent instructions from the supervisory system.

7. The failure of the communications network does not automatically shut down the plant's process controls, and if connections are restored, the operator can resume monitoring and control. Certain essential systems will be equipped with dual redundant data highways, which will be connected via multiple paths.

8. Human-machine interface (HMI): The human-machine interface (HMI) is the supervisory system's operator window. It graphically displays plant information to operating employees in the form of replica schematics, which are graphical representations of the plant under management, as well as alarm and event recording pages.

9. The HMI is connected to the SCADA supervisory computer, which feeds live data into the replica of diagrams, warning alerts, and tracking graphs. In many setups, the HMI serves as the operator's graphical user interface, collecting data from external devices, creating reports, performing alarming, and sending notifications, among other things.

10. A graphical plan is usually included in the HMI package for a SCADA system, which the operators or system maintenance people use to change the way these points are represented in the interface.

Types of SCADA systems:

1. Monolithic SCADA Systems
2. Distributed SCADA Systems
3. Networked SCADA Systems
4. IoT SCADA Systems

1. Monolithic SCADA Systems

Minicomputers are employed in these types of systems. When standard network services are unavailable, various systems can be developed.
These systems can be designed as stand-alone systems without any connections to other systems. A backup mainframe can be used to collect data from all RTUs. These first-generation systems' main activities are limited to signalling processes in crisis situations and observing sensors.

2. Distributed SCADA Systems

SCADA systems that are distributed are referred to as second-generation systems. By connecting to a local area network, the control functions can be distributed among multiple systems. Real-time data and command processing can be shared to accomplish control activities.
The scale and expense of each location are decreased in these systems, but there are no consistent network protocols. Because the protocols were secret, few people were aware of the SCADA system's security during installation, and this element was mainly overlooked.

3. Networked SCADA Systems

SCADA systems that are networked are also referred to as third-generation systems. The WAN system, which uses data lines or phones, can be used to network, and communicate current SCADA systems.
Ethernet or fiber-optic connections can be used for data reception and transmission nodes. This type of SCADA system employs a PLC to change and monitor the flagging activities only when they are required.

4. SCADA Systems for the Internet of Things:

SCADA systems that are networked are also referred to as third-generation systems. The WAN system, which uses data lines or phones, can be used to network, and communicate current SCADA systems.
Ethernet or fiber-optic connections can be used for data reception and transmission nodes. This type of SCADA system employs a PLC to change and monitor the flagging activities only when they are required.

Application of SCADA Systems

SCADA networks are widely used in today's businesses to monitor and study real-time data, control industrial operations, and connect with devices. Because SCADA systems comprise both hardware and software, they are critical for industrial enterprises. As a result, SCADA security is critical in industries.

SCADA Security:

SCADA security refers to the protection of SCADA networks that are built with computer hardware. Power, oil and gas, and other SCADA networks are used by some of the systems. Because of the importance of these networks in ensuring the security of SCADA systems, corporate and government companies have adopted efforts to protect them.

We will look into IoT SCADA systems:

How do IoT and SCADA work together?

Whilst SCADA technologies are common in industrial systems, the Internet of Things (IoT) offers capabilities and functions where SCADA stops off.

Because skilled hacker groups are likely to target SCADA and IIoT (Industrial Internet of Things) technologies and their overall system architecture, they confront cybersecurity issues. Control systems for industrial applications are also a popular target for government-sponsored hackers, posing serious security concerns for SCADA and IoT industrial control systems.

4.2 Cyberthreats to SCADA and IoT Systems:

SCADA systems are typically used to manage Industrial Control Systems (ICS), which in turn manage machines and other industrial equipment in industries such as oil and gas production, water and power utilities, pharmaceutical and medical, food service, automobile and airliners production, and durable goods manufacturing. The same can be said for industrial IoT networks, which are rapidly growing across a variety of industries.

These are typically vital industries that run complicated industrial equipment networks that span continents. If your company uses a SCADA or IoT control system, you should be aware that cyber-attacks can come from three different directions:

- Hacking groups who seek to infect your computers with ransomware.
- Competitors who engage in unethical industrial espionage.
- In a more sophisticated scenario, nation-state actors are wanting your sensitive data or aim to take over your business-critical production management systems.

Other attack tactics include internet approaches and spear-phishing techniques, as well as Trojan virus spreading via portable devices like infected USB sticks.

Typical Attack Descriptors:

Other attack channels include exploiting vulnerabilities such as: With the majority of industrial locations having at least one remotely accessible equipment, other attack vectors include exploiting vulnerabilities such as:

1. Using a serial interface to connect to a device.
2. For firmware, pre-set passwords or SSH keys are used.
3. Passwords in plain text are being intercepted throughout ICS networks.
4. There are no policies in place to prevent accounts from being locked out.
5. Alteration of a device's code execution cycle to gain access to sensitive data.

4.3 Protecting SCADA, IIoT and IoT Systems:

The President's Critical Infrastructure Protection Board in the United States has issued suggestions for increasing SCADA cyber security, emphasizing the necessity of protecting industrial control systems.

The following procedures should be included in a working cyber-security policy to secure your SCADA, IIoT, or IoT networks:

1. Prevent unwanted access to systems and subsystems by securing the boundaries.

2. Reconfiguring all known flaws and upgrading all installed software.

3. Accessibility to fundamental networking equipment and control modules is restricted both logically and physically.

4. Having a network connection monitoring solution in place.

5. Antivirus and firewalls should be enabled at all places where IoT networks connect to public networks like the Internet.

6. To verify that the system files are not manipulated by an attacker, use integrity of data checking software.

7. Implement redundant networking solutions for both hardware and software to ensure redundancy for important components.

4.4 Challenges to Secure SCADA systems in IoT-Cloud Environments:

Several risks in these environments could allow malware to infect SCADA systems, some of which are described below.

1. Device inputs and data can be tampered with, detected, misplaced, or disguised during communication since SCADA systems rely on cloud communication.

2. Network links between SCADA systems and the cloud could open backdoors into the ICS, which attackers could subsequently exploit.

3. Cloud-based SCADA systems have the same hazards as traditional SCADA systems.

4. Because the same cloud can be accessed by multiple clients, data on the cloud is only isolated internally.

5. Attackers can simply search and abuse SCADA systems apps that are hosted in the cloud.

6. SCADA systems use Modbus/TCP, IEC 40, and DNP3 for control and automation, but some of these protocols lack security.

7. Instead of proprietary solutions, SCADA systems use commercial off-the-shelf solutions.

8. SCADA systems do not have enough security controls.

9. In IoT device operating systems, unnecessary services and default factory settings cause setup issues.

10. Software problems in IoT device operating systems are caused by memory corruption and weaknesses in evaluating input data.

11. Configuration issues such as parameter manipulation and lack of encryption can occur when third-party software is utilized for IoT devices.

12. Individual cloud and external service providers have their own security flaws.

Few threats to SCADA systems in IoT-cloud context are listed below:

1. Advanced Persistent Threats (APTs):

APTs are network attacks in which an unauthorized user uses zero-day attacks to obtain access to a system to steal data rather than inflict damage.

2. Data Integrity:

When the original data is destroyed, data integrity is lost. This can occur through a variety of methods, including reduced computational methods or surveillance.

3. Man-in-the-Middle (MITM) Cyberattacks:

Spoofing and sniffer attacks are two attacks that can readily be launched as a result of a man-in-the-middle attack. A spoofing attack occurs when a software or an individual impersonates another program or person in order to gain unauthorized access to a system or network. In a sniffing attack, the intruder watches all of the communications that are sent and all of the actions that are taking place.

4. Replay Attacks:

A replay attack is a network assault in which a valid message containing some valid data is repeated; in some situations, the message may repeat itself. When a replay attack delays messages sent to physical devices, it affects the performance of SCADA systems and can be a major hazard.

5. Denial of Service (DoS) Attacks:

The goal of a DoS attack is to prevent the intended user from accessing a service. These cyberattacks can be carried out in a variety of ways, including DoS and DDoS. These attacks, at their most basic level, overburden computer resources to the point where the machine is unable to perform its intended activities.

4.5 Best practices for securing IoT-Cloud based SCADA systems:

1. Network Segregation:

This technique introduces security tools that surround each network, effectively segregating and monitoring network activity and preventing policy breaches.

2. Monitoring and Analysis:

The computers in SCADA systems conduct vital duties, which can make the systems complicated. Because of the growing frequency of attacks, it is necessary to regularly monitor and analyze the operations carried out by these computer systems.

3. Log Analysis:

Almost all computer software and devices, such as software applications, networking equipment, applications, and other sophisticated programmable devices, keep monitoring tools. Debugging, compliance checks, scientific examination, and intrusion detection all rely on these logs. Many assaults can be identified and controlled using these data. This type of log analysis is common.

4. File integrity monitoring:

File integrity analysis is conducted to ensure that some software and operating systems are safe to use. The most commonly used verification method is cryptographic checksums. Checksum verification methods make it simple to distinguish between harmful (black lists) and permissible (white lists) files. Host-based IDS also supports checksum techniques.

5. Network Traffic Analysis:

Hazardous actions can occasionally be spotted by performing network packet analysis while monitoring the network. Behavioural or pattern analysis can also be used to detect malicious actions. Network analysis can only detect the number of network packets or the destination for complex malware, where the information is concealed inside covert channels.

6. Memory Dump Analysis:

Memory dump analysis can detect both known and undiscovered harmful behaviour within an operating system's memory. A vulnerability system can evaluate many forms of memory dumps using modern technology. This form of analysis makes it simple to spot hidden processes and system libraries, which aids in the detection of sophisticated attacks and intrusions.

7. Constant Updating and Fixing:

IoT-cloud SCADA systems rely on third-party software and keeping this software up to date is a headache. Unexpected faults in such software can lead to attackers being able to execute arbitrary code. It's a good idea to keep up with the latest security news and follow the best practices for updating and patching this key infrastructure software.

8. Actively Evaluating Security vulnerabilities:

The system design influences its security level to a great extent. Continuous monitoring and vulnerability testing can readily uncover unknown flaws in cloud systems.

THE THREAT MODEL FOR IOT

The detection and development of a list of possible threats are referred to as a threat model. Threat models can include both physical safety and digital protection, which are inherent in cyber-physical structures.
The process of detecting essential assets and blocks involves splitting the production phase supply chain into usable blocks and listing the assets in those blocks.
This may include, in addition to risks of attacks, accidental events that may affect security, safety, and efficiency as a result of errors in managing the growing complexity of systems brought on by the addition of IoT.
Risk evaluation methodology should measure the relative importance of risks based on the domain's risk level and enforce actions to secure the various stages of the supply chain. The purpose behind cyberattacks should also be considered to identify cost-effective defences and security controls. Furthermore, a large number of IoT components demonstrate a lack of responsibility for the tasks they perform. This is due to the lack of logging in most IoT devices due to hardware limitations or extra costs. A risk assessment for the entire IoT supply chain setup should be performed to identify components where monitoring is needed.
While evaluating the attack vector for the product, a threat model must be created during the design process. All threats to the product should be rated following the CVSS guidelines, which consider the attack vector, complexity of the attack, and probability of occurrence, among other factors. This aids in risk prioritization and establishes a foundation for developing a protection plan for the product.

There are several forms of threat modelling, and three factors can differentiate them:

1. The logical object under consideration.
2. The stage of the device life cycle (for example, modelling protection for software during its initial design versus modelling security for off-the-shelf software that has already been implemented).
3. The threat modelling's target:

- **Software threat modelling**, which is threat modelling conducted during software design to minimize software vulnerabilities, is a common type of threat modelling. For performing software threat modelling, there are numerous proven methodologies. Another type of threat modelling is device threat modelling, which is threat modelling conducted for operating systems to enhance their overall protection. In comparison to software threat modelling, device threat modelling is more informal and ad hoc.
- **Data-driven framework threat modelling** is a subset of threat modelling that focuses on protecting specific data types within systems.

The complex essence of defense necessitates threat modelling. Security would be impossible to solve if it were a one-time job. Unfortunately, the attack side is ever-changing; new weaknesses are found, new attacks are created, and new threats emerge.
Long-term shifts occur as well—new groups of vulnerabilities are found, attacker motives shift, and other transitions occur over time. Security controls are continually improved and upgraded, new types of security controls are introduced, and so on. Change is unavoidable; for example, when one class of vulnerabilities becomes well remedied, attackers easily find another group of vulnerabilities that are not as well minimized to exploit, and defenses adjust security measures appropriately.
Instead of relying solely on "best practice" generic guidance, data-centric device threat modelling enables organizations to understand the security needs of each case of interest. Best practices for operating systems and individual applications, such as securing a web server (host) or web server apps, are now well established in organizations. What is much more difficult for companies to handle is deciding how to protect a specific piece of data. It is not so much that protecting data is challenging because historically, security experts, system managers, and those in charge of securing operating systems have concentrated on securing systems rather than data.

5.1 How to Carry out Threat Modelling

Although there are numerous approaches for threat modelling, the research is usually carried out by taking the following topics into account:

1. Definition of the system: This provides a description of the method and how it accomplishes its goal and fulfils its use cases. Any industry-specific security criteria and any limitations or assumptions about the system in the target market must be taken into account.

- Describe the system's lifecycle: This is a black box overview covering aspects such as how the system is produced, designed, deployed, and how it approaches to stop, and the various entities involved in each level.
- Describe the system's fundamental operations, usually in pictorial blocks, and show how knowledge flows from one block to another.

2. Determine the trust boundaries: Identify the security or trust limits beyond which security within an object of study can be evaluated and define the trust relationships between the objects. Determine the flow of knowledge through the trust boundaries. The research must consider the method applied in its larger sense, even though it is a black box.

3. Determine who the stakeholders are: A stakeholder is an individual, party, or organization that assigns a monetary value to the system based on its essential assets. The list of stakeholders is typically extracted from business protection criteria and the system's lifecycle.

4. Determine the vital assets that must be safeguarded: Determine the properties that must be safeguarded and the business rationale for doing so. Key properties of assets, such as confidentiality, honesty, or availability, may be jeopardized by attackers. Assets may be a direct target for attackers looking to hack the infrastructure. However, some properties, such as encryption keys, can serve as stepping stones to the system's compromise.

5. Determine attack surfaces: An attack surface is the number of the various points (the "attack vectors") from which an unauthorized user can communicate with the device. Input and output ports, APIs, and computing side effects such as timing, and power consumption, are examples of attack surfaces. As a result, the attack surface is inextricably linked to the defense boundary. The attack surface is determined by the threats and adversarial tools under consideration in the study.

6. Make a model of your opponent (threat actor): The adversarial model reflects the levels of expertise, skills, and resources that an attacker might use to damage the system's properties. These are extracted from use cases, business protection specifications, attack surfaces, and adversaries to manipulate the device.

7. Determine possible future risks: Examine the attack surfaces, and the information flows across the confidence boundaries defined in the device definition. For example, the Microsoft STRIDE model can be extended to attack surfaces and the use of attack vectors as a means of compromising an asset. In this research, knowledge of adversarial models is important.

8. Threats that have been detected are subjected to a risk assessment: The threat's probability must be calculated. The effect of each hazard on the system and organization must then be calculated. These two factors are added together to determine the overall risk of the attack.

- Mitigation actions: Determine what should be done with each hazard based on the danger. For example, it may be appropriate to reduce the threat to an acceptable level, admit that it is not a danger, remove the feature that causes the threat, or pass the threat to a more suitable group.
- Contingency planning: Countermeasures are typically captured at two levels: security objectives, high-level descriptive goals for mitigating threats, and mitigations, low-level descriptive goals for mitigating threats. Security Functional Requirements are low-level prescriptive features or design strategies that must be introduced to achieve the mitigation specified in the security objectives.
- There may be residual risks, and it may be appropriate to repeat the steps.

5.2 Data-centric Threat Modelling

Data-centric system threat modelling combines attack and protection side details for data of interest in a structured model that aids in vulnerability analysis, decision making, and change management.

Step-1

The first step is to classify and define the relevant system and data. The framework and data should be strictly specified, of a specific logical collection of data on a specific host or small group of closely related hosts and devices. If the system and data have been identified, they must be characterized, which means comprehending the system's operation and useful to the degree required for the organization's data-centric system threat modelling approach. At an absolute minimum, characterization should include the following:

The system's approved data storage locations included but not limited to:

- Storage, available inside the device boundaries where data is static.
- Transmission refers to all methods by which data can be transferred across networks between system components and across system boundaries.
- An execution environment in which the data is stored in a local memory during runtime while a virtual CPU processes data.
- Input like data entered using a keyboard or touchpad.
- Output like data displayed on a laptop or voice confirmation.

There must be a fundamental understanding of how data moves inside the system between approved locations. For example, a file can be generated in memory and only written to storage when the user instructs the device. Depending on the system's sophistication, achieving this can call for an understanding of the system's roles and processes, users and implementation scenarios, workflows, trust expectations, and other system-related people, systems, and technology.
Among the security objectives, certain goals are more relevant than others in many ways. Alternatively, organizations may focus on a single target with a specific threat model.

The people and processes who are authorized to access the data in a way that could affect the security objectives. For example, if an enterprise has chosen anonymity as its sole goal for a specific threat model, the approved persons and processes should include all customers, managers, programmers, providers, and so on that are permitted to read the data.

Step-2

The second step entails defining possible attack vectors that may be used to undermine one or more of the established security goals for one of the authorized data locations. If the attack vectors have been defined, it could be possible to use only a selection of such vectors in the hazard model. While using all attack vectors is ideal, there are often too many to solve with minimal resources. Consider the relative risk of the attack vector being used, as well as the possible effect of a successful attack.

Step-3

The third step of the approach is defining and recording security management changes that will help minimize the risk associated with the attack vector that is fairly realistic to implement with each attack vector chosen in Step 2. It is important to note that it is not mandatory to list any single applicable control, such as maintaining a compliance program and rules, since these controls may still affect the whole enterprise and are not usually tailored to account for a specific attack vector. Next, approximate how effectively each chosen security control change will solve the manipulation of each relevant attack vector.

This may be as straightforward as assigning a minimal, medium, or high level of efficacy or as nuanced as calculating the proportion of attacks against the attack vector that this mitigation will prevent. Whatever strategy is used, it must be consistent through mitigations and attack vectors. Estimating the negative consequences of each security control change is the inverse of estimating the effectiveness. Cost and decreases in functionality, usability, and efficiency may be factors to consider. These can be especially difficult to predict for potential mitigations reliably, so it might be best to create very preliminary calculations using a basic low/medium/high style scale exclusive to the organization.

Step-4

The methodology's final step is to review all the characteristics reported in the preceding stages, which collectively form the hazard model, to aid in assessing the efficacy and efficiency of each protection management option against the chosen attack vectors. To assume that control should be used because it reduces risk is much too straightforward. Security controls, in addition to the financial costs of procurement, execution, and management/maintenance, may have a detrimental effect on reliability, efficiency, and efficiency, among other factors. Any evaluation of security measures should take into account all important related variables. The most difficult aspect of hazard model research is deciding how to take all these features into account at the same time. A specific attribute, such as annual management, can be easily compared across attack vectors and mitigations. However, comparing the entire set of characteristics for one attack vector to the entire set of characteristics for another attack vector is extremely difficult.

Such comparisons, however, are crucial in deciding how risk can be cost-effectively minimized across all attack vectors with a reasonable negative impact on the organization's performance.
Each enterprise must decide how to compare the characteristics of each attack vector control pair as a foundation for comparing attack vector and protection control characteristics. One method for making these contrasts easier is to assign ratings and weightings to each characteristic. Narrative accounts of hazard consequences, for example, may be translated to numerical values on a three-point scale. In addition to the low, medium, and moderate scores, three-point scales could be used for other characteristics. Also, complex features, such as price, may be reduced to a single scale. The company must consider the proportional weights of each characteristic in addition to awarding ratings to each characteristic's potential values or significance ranges. Perhaps the ability to repel attacks is regarded as much more critical than other attributes. If this is the case, it may be communicated by doubling or tripling its score. Similarly, the other traits should be given a multiplier that increased or decreased their scores or kept them constant. The company will then sum up the outcomes after applying the multipliers, yielding a relative score for each attack vector control combination.

5.3 Why IoT Threat Modelling Matters

It is common knowledge that IoT systems lag in terms of network and information security because of the following factors:

- Lax manufacturing standards
- Devices that lack the computing horsepower
- Devices that lack safe storage space

If a single device is adequately protected, unsecured devices can remain in the organization's ecosystem. This completely circumvents the complexity and breadth of IT security departments, exposing entire networks to data breaches. These IT security loopholes can be discovered using architecturally dependent IoT hazard modelling.
A company will quickly lose control of its IoT ecosystem attack surface if it does not have clear IoT protection.

Architectural IoT Threat Modelling Example

IoT-based aircraft system's vulnerability model map can be studied for the numerically largest source of cyber threats to the aircraft, excluding IoT systems for the time being. Upon examining these attacks, it reveals that they mainly threaten endpoint users who use their mobile phones or laptop computers while flying. Such risks are thus of low priority for the aircraft's defense.
Considering the IoT aircraft device threat paradigm, the risks posing the greatest danger to the actual aircraft originate from the integrated IoT systems. These devices are used to track and automate essential elements of the physical aircraft environment.

The following basic threats have been described as a result of architecturally-based IoT hazard modelling:

- Action Spoofing
- Device Hijack
- Denial of Service
- Faking the Data Source
- Insecure Wi-Fi Channel
- Manipulating Writable Configuration Files
- Targeted Malware
- Wi-Fi Jamming

5.4 Threat Modelling for Device-level Security

IoT device-level protection entails safeguarding the network at the level of specific computers in order to provide a secure atmosphere for consumers. To create a protection scheme that effectively safeguards the network: a device-level inspection must be performed, as well as the detection of essential vulnerabilities that occur in particular systems.

Threat Modelling Methods	Features
STRIDE	• Aids in the identification of appropriate countermeasures • An advanced method • Simple to use, but it takes time • Has programmed modules • Has incomplete and ambiguous documents
PASTA	• Aids in the identification of appropriate countermeasures • Contributes explicitly to risk control • Encourages stakeholder engagement • Has built-in threat reduction prioritisation • Is time-consuming but has extensive documentation
CVSS	• Has constructed threat reduction prioritisation • Produces reliable results when replicated • Has programmed modules • Score measurements are opaque

Threat Modelling Methods	Features
LINDDUN	• Encourages stakeholder engagement • Has built-in threat reduction prioritisation • Is time-consuming but has extensive documentation
Attack Trees	• Aids in the identification of appropriate potential solutions • Produces reliable results when used repeatedly • Simple to use if you already have a detailed understanding of the method
Persona non Grata	• Helps to classify applicable countermeasures • Directly contributes to addressing risk • Produces reliable results when replicated • Detects only a portion of risks
Security cards	• Encourages stakeholder engagement • Detects unusual threats • Produces a lot of false alarms
htMM	• Has built-in threat reduction prioritisation • Encourages stakeholder collaboration • Produces accurate results when replicated
Quantitative TMM	• Has built-in threat reduction prioritisation • Encourages stakeholder collaboration • Produces accurate results when replicated
Trike	• Encourages stakeholder engagement • Detects unusual threats • Has built-in threat reduction prioritisation • Encourages stakeholder collaboration • Has programmed modules • Has incomplete and ambiguous documents

Threat Modelling Methods	Features
Vast Modelling	• Encourages stakeholder engagement • Detects unusual threats • Has built-in threat reduction prioritisation • Encourages stakeholder collaboration • Has programmed modules • Has incomplete and ambiguous documents • Produces accurate results when replicated
OCTAVE	• Encourages stakeholder engagement • Detects unusual threats • Has built-in threat reduction prioritisation • Encourages stakeholder collaboration • Is designed with scalability in mind • Has incomplete and ambiguous documents • Produces accurate results when replicated

Table 11. Different Threat Modelling Methods

PASTA Model

The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat-modelling framework that contains seven stages, which are as follows:

- Define objectives
- Define technical scope
- Application decomposition
- Threat analysis
- Vulnerability and weakness analysis
- Attack modelling
- Risk and impact analysis

LINDDUN Model

A LINDDUN (Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of Information, Unawareness, Noncompliance) model focuses on privacy issues that can be used to secure data.

LINDDUN begins with a system Data Flow Diagram that describes the system's data flows, data stores, operations, and external entities. LINDDUN users define a threat's applicability to the structure and create threat trees by iterating over all model components and evaluating them from the standpoint of threat categories. It is divided into six stages.

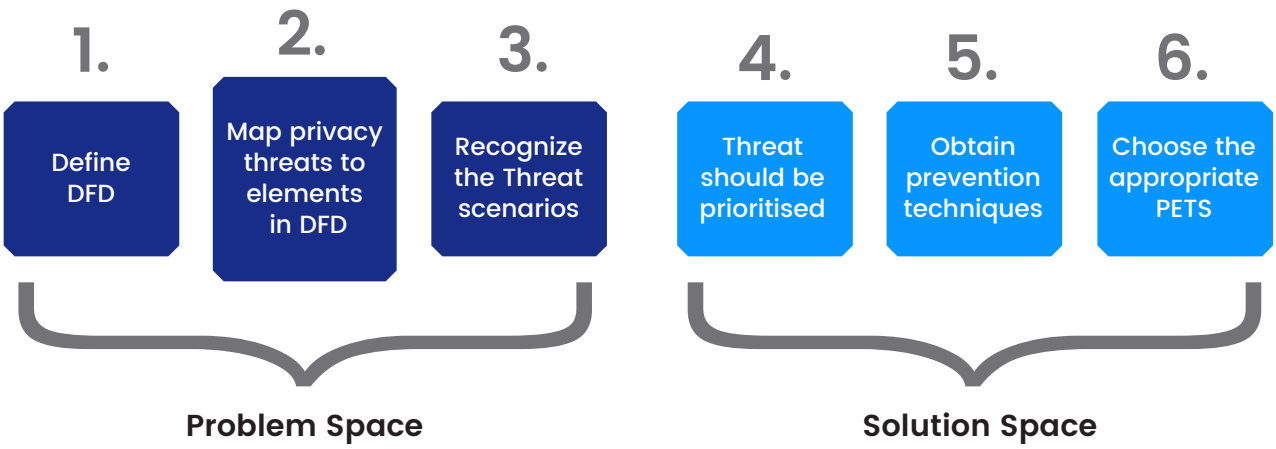


Figure 18. Data-flow Diagram of LINDDUN Model

CVSS Model

The Common Vulnerability Scoring System (CVSS) captures the principal characteristics and produces a numerical severity score. The CVSS provides users with a common and standardized scoring system within different cyber and cyber-physical platforms. The CVSS Model consists of three metrics, namely, Basic, Temporal, and Environmental.

Base Metric Group		Temporal Group	Environmental Metric Group
Exploitability metrics	**Impact metrics**		
• Attack vector • Attack complexity • Privileges required • User interaction • Scope	• Confidentiality Impact • Integrity Impact • Availability Impact • Scope	• Exploit Code Maturity • Remediation level • Report confidence	• Modified base metrics • Confidentiality requirement • Integrity requirement • Availability requirement

Table 12. CVSS Model Metrics

Attack Trees Model

Attack Trees are diagrams that show attacks on a machine in the shape of a branch. The attack aims to reach the tree's root through the leaves. Its tree defines each target. As a result, the device threat analysis generates a series of attack trees. Supervisors may create attack trees and use them to make security decisions, decide whether networks are vulnerable to attacks, and analyze particular types of attacks.
This approach has often been used in conjunction with other methods and systems such as STRIDE, CVSS, and PASTA in recent years.

Persona non Grata Model

Persona non Grata (PnG) is concerned with the motivations and abilities of individual attackers. It characterizes consumers as archetypes that can abuse the machine and forces researchers to see the system from accidental use.
PnG can aid in the visualization of threats from the opposing side and be useful in the early stages of hazard modelling. The plan is to add a technical specialist to a possible machine attacker and investigate the attacker's abilities, motives, and aims. This research assists the specialist in comprehending the system's flaws from the perspective of an attacker.

Security Cards Model

In order to promote threat-discovery operations, a deck of 42 cards is used: Human Impact (9 cards), Adversary Motivations (13 cards), Adversary Resources (11 cards), and Adversary Methods (11 cards) (9 cards).

Human impact	Adversary's Motivations
• The biosphere • Emotional well being • financial well being • Personal data • Physical well being • Relationships • Societal well being • Unusual impacts	• Access or convenience • Curiosity or boredom • Desire or obsession • Diplomacy or warfare • Malice or revenge • Money • Politics • Protection • Religion • Self-promotion • World view • Unusual motivations

Table 13. Security Cards Model

Adversary's resources	Adversary's Methods
• Expertise • A future world • Punishment • Inside capabilities • Inside knowledge • Money • Power and influence • Time • Tools • Unusual resources	• Attack coverup • Indirect attack • Manipulation or coercion • Multiphase attack • Physical attack • Processes • Technological attack • Unusual methods

Table 13. Security Cards Model

htMM (Hybrid Threat Modelling) Method

It comprises SQUARE (Security Quality Requirements Engineering Method), Security Cards, and PnG operations. The method's focused characteristics include no false positives, missed risks, and a clear finding independent of the person performing the hazard modelling and being cost-effective.

The method's key steps are:

1. Identifying the device to be threat-modelled.
2. Use the Security Cards under the developer's recommendations.
3. PnGs that are impossible to occur should be removed.
4. Use the tool to help summarize the findings.
5. Maintain a systematic risk assessment process.

Quantitative TMM Model

This hybrid approach combines assault trees, STRIDE, and CVSS approaches in a synergistic manner. It seeks to resolve a few pressing issues through threat modelling for cyber-physical systems with complex interdependence among their components.
The first stage in the Quantitative Threat Modeling Method is to build component attack trees for each of STRIDE's five threat groups. This behaviour demonstrates the interdependence between attack types and low-level object attributes. Following that, the CVSS procedure is used, and scores for the tree's components are measured.

Trike Model

Trike, like many other processes, begins with the definition of a procedure. The analyst creates a requirement model by listing and comprehending the system's actors, properties, planned behaviour, and laws. This move generates an actor-asset-action matrix, with columns representing properties and rows representing actors.

Each matrix cell is divided into four segments, one for each CRUD operation. The analyst assigns one of three values to these cells: permitted action, disallowed action, or action with laws. Each cell has a rule tree attached to it.

A Data Flow Diagram is created after the specifications have been established. Each variable corresponds to a group of actors and properties. The researcher iterates through the DFD, identifying risks that fall into one of 2 groups: elevations of privilege or denials of service. Each discovered threat is added to an attack tree as a root node.

Trike uses a five-point scale for each operation, depending on its likelihood, to measure the risk of attacks that can impact properties through CRUD. Actors are scored on a five-point scale based on the threats they are expected to pose to the asset. Actors have graded on a three-dimensional scale: always, sometimes, or never, for each move, they will take on each asset.

Vast Modelling Model

Threat Modeler, an advanced threat-modelling tool, serves as the foundation for the Visual, Agile, and Simple Threat (VAST) Modeling process. Its scalability and reliability enable it to be implemented across large enterprises' entire networks to deliver actionable and consistent outcomes for various stakeholders.

Recognizing organizational gaps and challenges among development and infrastructure teams, VAST necessitates developing two types of systems: application threat models and operational threat models. Process-flow diagrams are used in application hazard models to reflect the structural perspective. DFDs are used to construct operational vulnerability models from the perspective of an intruder.

OCTAVE Model

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach is a risk-based operational cybersecurity analysis and preparation method.

The OCTAVE Model is divided into three phases:

1. Create hazard profiles based on assets.
2. Determine the instability of the networks.
3. Create a defense agenda and action plans.

OCTAVE is primarily concerned with evaluating operational threats and does not consider technical risks. Its three key components are organizational risk, security policies, and technology.

5.5 Defining Threat Model for IoT Networks

Threat Model for Healthcare

A threat model for IoT health devices is created by adapting general threat modelling steps such as

(a) identifying IoT device assets,
(b) identifying device access points,
(c) identifying threats.

Individuals who use or promote the use of these instruments are referred to as stakeholders. They will also use this system to determine the security risks associated with using some of the systems depicted in the model.
Medical practitioners may also use the framework to learn about technologies that have been recommended for their patients' use. Researchers may also test the device based on the kind of study they are doing.
All system information, such as device risks and ratings, will be calculated and stored in a database. The developer will be the professional in charge of managing the infrastructure by doing routine system changes such as installing new equipment and risks and recalculating risk ratings.

Identifying Threats

A vulnerability is a potential risk that exploits a system's or device's vulnerabilities in order to gain unauthorized access or inflict damage to the system or device. Threats can occur as a result of the actions of legitimate users of the computer or system who have permitted access to the system, as well as unlawful or unauthorized users of the system or device. We will use the STRIDE model, which categorizes risks into six categories: spoofing, tampering, repudiation, information leakage, denial of service, and privilege elevation.

Type of threats	Information
Spoofing	Threatening to access and use another user's credentials, such as username and password, without permission.
Tampering	Threat behaviour aimed at altering data in transit between two computers over an open network, such as the Internet, and maliciously changing/modifying persistent data, such as persistent data in a database.

Type of threats	Information
Repudiation	The threatening activity aimed at carrying out criminal activities in a system that lacks the capacity to track them down.
Information disclosure	Threatening action to read a file to which you have been denied access or to read information assets.
Denial of service	Threat directed at denying access to legitimate users, such as by briefly rendering a Web server inaccessible or obsolete.
Privilege Escalation	Threat designed to obtain exclusive access to resources in order to obtain unauthorized information or breach a system.

Table 14. STRIDE Model to Identify Threats

Spoofing

Email spoofing is used as a trick to share sensitive information or steal users' credentials. Often, spoofed emails are submitted by changing the sender's name or email address. In addition, the content of the message is often structured in such a manner that it seems legitimate to the receiver. Countermeasures may include:

- Good authentication: A strong password policy or multi-factor authentication methods may be used to authenticate the user to the device.
- Encryption: All passwords must be secured, and it must be guaranteed that no credentials are sent over the wire in cleartext.

Tampering

An attacker tampers with data in transit or at rest. Countermeasures include:

- Strong authorization: Appropriate access management systems, such as role-based access control, must be deployed with the least privileges and division of duties rules in place. Users must be assigned permission with the bare minimum of rights.
- Data hashing and signing: In order to ensure the validity of the data, all sensitive data must be hashed and authenticated.
- Secure communication links: The communication links between device components must be protected by protocols that maintain message integrity and privacy.

Repudiation

- Authorized users engage in unlawful activities, and the device is unable to track them down; other people are unable to verify this. Countermeasures include:

  - Secure Audit Trails: Both confidential data and events must be logged and registered.

Information Disclosure

Raw evidence or medical documents are being leaked. Countermeasures include:

- Strong authorization: Make certain that an effective access management system is in place and that only approved users have access to data.
- Encryption: Ensure that all confidential data is encrypted (while in storage or in transit) and that only approved users have access to it.
- Safe communication links: Make certain that all communication links are protected by protocols that ensure message security.

Denial of Service

An attacker is jamming the hospital environment. Countermeasures include:

- Mitigating this type of protection risk is difficult since remedies are heavily dependent on a variety of variables.

Elevation of Privilege

Attackers obtain access to authentication networks by masquerading as trustworthy individuals. Countermeasures include:

- A proper authorising process is needed.
- The principle of least privilege requires that all permitted users have the bare minimum of privileges and access.

Rating Identified Threats

Threats are rated using scales representing high, medium, and low. A danger ranked as high poses a significant risk to the system or the device software programme and must be addressed as soon as possible by introducing suitable countermeasures. A medium-risk threat must also be tackled, but not as urgently as a high-risk threat. A danger classified low may go unaddressed because it does not necessitate the same level of urgency as the other two threat levels. We may use the DREAD model for scoring.

Following the rating of the risks, a risk score is determined using the formula
Risk Score = (Damage + Reproducibility + Exploitability + Affected users + Discoverability)/5.

Rating	High	Medium	Low
Damage potential	The intruder can get full trust permission, operate as an admin, and share data by subverting the security framework.	Leak delicate information.	Leak trivial information.
Reproducibility	The attack can always be replicated and requires no time.	The attack can only be replicated with a time frame and a specific situation of race.	Even knowing the security breach, the attack is very hard to repeat.
Exploitability	The attack might be done in a short period by a beginner programmer.	A qualified programmer could attack and then repeat the steps.	The attack requires a highly skilled person and a thorough understanding to use every time.
Affected users	All users, default settings, key clients.	Non-default setup for some users.	Very small proportion of users, darkness; affects anonymous users.

Rating	High	Medium	Low
Discoverability	The attack is explained by the published facts. In the most frequently used function, the weakness is identified and is very apparent.	The vulnerability is a rare part of the product and should be experienced by only a handful of users.	Some people would need to think about the wrong use. The bug is dark, and users are unlikely to determine the potential for damage.

Table 15. DREAD Model Threat Rating Scheme

Threat Model for Smart Home Devices

As a first step, look at the grid elements of the Data Flow Diagram that specifically fall within the domain. They are shown as complicated systems.

The following table, for example, indicates including the Smart Meter instance as a complex mechanism with three data stores and the related data flows. As a result, the smart home pattern instance's instantiated feature "Energy Meter" is described in the Data Flow Diagram as a dynamic mechanism called Energy Meter. The data stores Energy Meter Keystore, Energy Meter Application Data, and Energy Meter Measurement Data. The second move is to consider elements inside the smart home essential from a security standpoint but cannot be aggressively modified because third parties supply them. They are represented as foreign bodies within the smart house.

All elements introduced in this stage must be segregated from those added in Step 1 using privilege boundaries. The explanation for this is that there are many players in the smart house. We examine the smart home's key elements typically supplied by a single party and associated subcontractors, such as energy providers and meter point operators. The level of confidence for parts that cannot be actively handled is separate from items that communicate within the smart home but are supplied by external, diverse parties. For example, the Smart TV, a component of the smart house, communicates with other components but is not included in the definition because an external vendor supplies it. As a result, it is added as a distinct external body distinguished by a privilege boundary.

The third move is to include the grid components, which are not part of the smart home but are also essential for stability.

We add the generic DFD with generic placeholders for the elements within the smart home and do not yet replace them with the instantiations indicated in the preceding table.

The items within the smart home supplied by third parties, on the other hand, are shown as external actors and will remain so in the study. All of these elements will be replaced by their instantiations at a later stage. The fourth step is to apply the smart grid pattern instance's grid element connections to the DFD and the grid elements that are not part of the smart house. Essentially, each grid element connection part of the scope is associated with at least one data flow. A grid element connection is included in the scope if at least one connected grid element is included. If it is unidirectional, it is mapped to a single data flow. Otherwise, it is associated with two data flows.

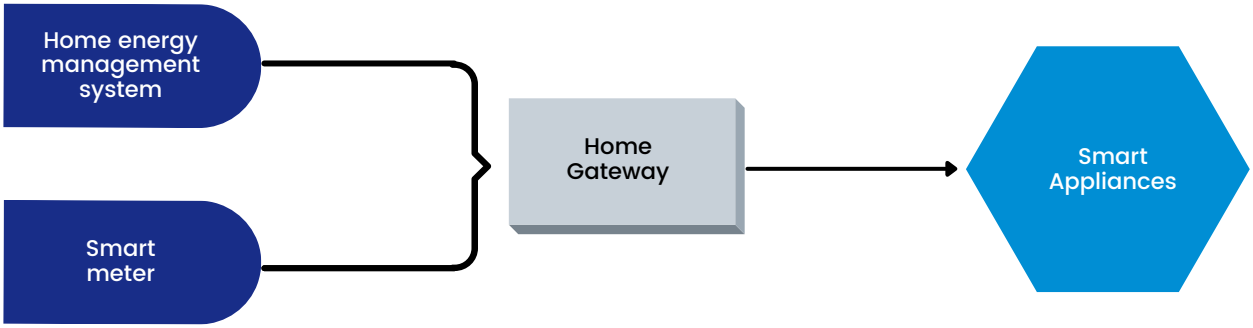


Figure 19. Data Flow Diagram (DFD) for Smart Home Devices

Refinement of the Initial DFD

The initial DFD, as modelled in Steps 1–4, can be refined further if necessary. In order to refine properties, data stores can be broken up, or core processes can be introduced. For instance, we added the process of Internet Routing to the DFD depicted above. The distilled assets' representation corresponds to the asset template outlined in Step 4. The Prosumer's contact with the EMS on his or her property. The Data Flow Diagram already captures certain facets of defense, which aids in identifying potential properties. Any part has a cryptographic Keystore, which stores any cryptographic information required for message signing and communication channel security. Billing data and consumer profile data, as well as personally identifiable information, are represented.

Identify Entry Points and Analyze Vulnerabilities

From the standpoint of an intruder, the properties listed in the preceding phases are important targets. Different entry points should be established with all properties in mind. Entry points describe a certain vulnerability that can be abused, resulting in an attack tree extending from the entry point to one or more properties. The diagram above depicts the various entry points. It should be remembered that entry points are elicited while the protection assumptions of each particular asset described in the refined asset specifications are taken into account.

If an aspect is a possible entry point, it depends on the attackers, their various motivations, and their skills. In this stage, various attacker classifications can be used. Within and outside the smart house, an exemplary range of expert attackers, including network and software attackers, is selected. Future studies may include a thorough examination of all attacker models, both physical and social engineering adversaries.

Network attackers are adversaries that have active access to a target network and can successfully eavesdrop and manipulate its communications. They have minimal computing power, time, and financial resources. They may be either registered users or external adversaries. It is assumed that they cannot break any cryptographic challenges, nor are they able to penetrate physical locks nor break software security measures.

Software attackers, on the other hand, are able to analyze, reverse engineer and compromise software systems. They are not capable of interfering in network traffic, nor are they able to penetrate physical security. They have limited computational capabilities, time as well as financial resources and can be both an authorized member of the system or an external adversary. To achieve alternative entry points, we apply high-level logic to each dynamic process to determine if the above intruder types will enter this specific process or not. If we cannot rule out the risk of an attacker gaining access to the mechanism in question, it's classified as a general entry point.

Further, for each step that has been assigned as a general entry point, we optimize the entry point & decide whether one of the possible attackers has the ability to manipulate each data flow from or to this process. If at least one attacker has access to the data flow in question, we mark it as an entry point. An attacker can choose individual entry points based on the properties he wishes to compromise.

Vulnerabilities and potential risks can be extracted from the elicitation of properties and entry points. This is accomplished in the next step by mapping entry points to properties and categorizing them using the STRIDE categorization. STRIDE refers to the following actions taken by an attacker: Spoofing is the act of tampering with data or code. Repudiation refers to the reasonable denial of having taken action, information

leakage of access-restricted data, and denial-of-service attacks. When an attacker's privileges are elevated, he or she enjoys greater capability and administrative authority.

Asset	Smart Meter
Reasoning	The calculation of the Smart meter affects billing, energy storage, energy forecasts for each segment and third-party value-added services.
External dependency	The smart meter partly relies on the Home Gateway to send accounting data to the Energy Management System.
Security assumptions	The Home Gateway and the link are secure and trustworthy.
Security notes	The MPO does not collect data on the Prosumer's energy use. The Smart Meter does not permit contact with the Prosumer. The energy management system acquires Billing data. The intelligent meter does not permit remote power shutdown.
Contains assets	Billing data, encryption keys and communication with others Message Verification.

Asset	Home Gateway
Reasoning	Internal and external connectivity via the Smart Home is dependent on the Home Gateway (HG). The HG cannot receive the billing data of the smart meter, control the actions of Smart Appliance and neither send and receive Billing Data feedback nor respond to demand-side management events without HG.
External dependency	The Home Gateway must be properly accessible and configured by the supplier.

Asset	Home Gateway
Security assumptions	Proper configuration means that IP addresses of the endpoint are right, authentication is enforced, and data transmission privacy is sufficient.
Security notes	The Home Gateway must be properly accessible and configured by the supplier.
Contains assets	The MPO must be informed of misconduct. Home Area Network Communication Keys.
Asset	**Profile Data, Billing Data**
Reasoning	Personally, Identifiable Information (PII) such as details on the profile (name, address, birthday) and Billing data provides a thorough insight into the PII's customs and affections.
External dependency	Billing data is based on the accuracy of the smart meter. Billing data aggregates are subject to aggregation.
Security assumptions	The measurements of the smart meter are precise. Algorithms are safe to aggregate.
Security notes	Physically stable, the cryptographic Keystore.

Table 16. Security Assumptions of Smart Home Assets

6.1 Introduction

There is a lot of Research and Development happening in IoT Security in several areas, such as Authentication, Authorization, Encryption, etc. The key research areas and the reasons why they are important are described in this section.

Even before receiving or transmitting data, device authentication must be triggered when the asset is added to the network for the first time. Embedded devices need not wait for users to enter the passwords needed to access the network, but they must be correctly identified before authorization can take place. Similar to how the user authentication mechanism allows a user to access the corporate network with a user- name and a password, machine authentication allows devices to access the network with a pair of credentials stored in a secure storage area. These authentication mechanisms are mostly referred to as Device-to-device (D2D) authentication, where authentication credentials are exchanged through a Machine-to-machine (M2M) channel. The resource-constrained design of IoT devices encourages lightweight approaches to maintain a sufficient degree of transmission performance. As a result, embedding a proper authentication protocol via circumspect design is critical from both a security and a transmission standpoint.

6.2 Confidentiality

Confidentiality is the blocking of access to non-public material when more than two parties have agreed to it. For example, the information on glucose readings a wireless glucometer sends to an automated insulin pump in a body area network must be safeguarded. Patient safety demands that the data should be safely stored and encrypted against unintentional or malicious tampering. There must be a verification mechanism to connect to a legitimate glucometer (and receive data from it) rather than an unauthorized device.
Proof of authorization certifies that a peer has the right to both coordinate with another peer and perform a specific action. In this case, a glucometer should allow data requests from an insulin pump and not from any other device; additionally, both the glucometer and the pump must be made by the same company. Also, the reset of the glucometer sensor should be carried out if the insulin pump has the appropriate authorization level.

What is Encryption?

Encryption is a means of securing the integrity of data. Encryption turns data, such as a folder or spreadsheet, into an unintelligible, scrambled file. Encryption preserves data by scrambling it and rendering it unreadable before the correct cypher and key are used to decode it. A cypher is a method of scrambling data using a mathematical algorithm.
The most significant barrier to encrypting applications is the device's simplicity, such as sensors. Furthermore, there could be a conflict in terms of the product's usability. However, to protect the anonymity and security of users, it could be worthwhile to enforce lightweight encryption in smartphones.
The network layer is the focus of current studies on encryption-based strategies for maintaining secrecy.

Encryption to protect data at rest in motion and in use

States of the Data

There are three different states of data, they are:

1. At Rest
2. In Transit
3. In Use

1. At Rest: If the data is at rest, then it means that it is located in media like files/flash drives/hard disks etc. and it(data) is not accessed.

2. In Transit: If the data is in transit, it means that it is moving from one location to another. It can take place through many means like messaging/emails etc.

3. In Use: When the data is accessed by a user, then, we can say that the data is in use.

Protection of the data

A. Protection of data 'At Rest':

One of the major ways to protect the data at rest is by different modes of encryption. The various useful modes of encryption are:

1. Full disk encryption: With this, the user has an advantage, the data can be accessed by the user with the login credentials, yet, we cannot protect the data once it is extracted from the device.

2. File-level encryption: Here, each file is protected. So, one must have the public key to access it.

3. Database Encryption: This allows for encryption and decryption in real-time. However, it protects the data only when it is at rest.

4. Protection through Digital Rights Management (IRM): Here, permissions will be given to the user, and the one who has full access can make the necessary changes to the file.

5. MDM (Mobile Device Management): This is the most useful when the mobile device is lost, we can control the access to applications on it.

6. DLPs (Data Leak Prevention): This allows for locating data in a network repository. However, it is protected only until the data is in the organization.

7. CASB (Cloud Access Security Brokers): We can give/deny access to anyone with this. The file is protected as long as it is in the cloud.

B. Protection of data 'At Transit':

Let us see the various ways to protect data in transit:

1. Email encryption: With tools such as PKI (Public Key Infrastructure), we can encrypt an email. With PKI, we can have a private key for ourselves as well as a public key for everyone else to access.

2. Managed File Transfer (MFT): This is the best way to secure transferring files. The file will be in a platform with an expiration date and one can open the link (if provided only) to access the docs.

3. DLP: This allows to spot malicious activities like sending (data in transit) data outside the organization and blocking it.

4. CASB: If one tries to download data that she/he is not given access to, this can block him/her from doing so.

5. In-transit protection with digital rights: We can protect data 'in transit' like forwarding/replying to emails.

C. Protection of data 'In Use':

To protect the data in use, controls should normally be put in place "before" accessing the content. For example, through:

1. Identity management tools: This concerns with the user, we can see who is accessing the file and when.

2. Conditional Access or Role-Based Access Control (RBAC) tools: Allows data access to the user based on his/her role and up to what extent they need access.

3. Through digital rights protection or IRM: We can deny access to the user once he/she has gained the access to the file (the user cannot edit if we don't want him/her to).

Challenges of Data Protection

A. At Rest:

1. There can be different copies of the data, they need protection too.

2. In mobile phones, sensitive data can be usually managed by many and we can't do anything about it as yet.

3. With cloud storage, because the key is in the hands of the provider and not the organization, we may lose control over it.

4. We need to make sure we have all the required security policies/patents, and not miss any in order to avoid complications.

B. In Transit:

1. There are many means of communication and we need to protect each of them separately. This is the same with the cloud too, there are simply too many cloud applications to protect.

2. Control at the receiving end: We almost can't control the receiving end because they have the access to the file and may decrypt it.

3. With the DLPs and the CASBs we have to be very clear about what we are protecting, and this is not always possible (based upon the organization).

Summary

Certain algorithms, such as the Advanced Encryption Standard (AES) and block cypher protect secrecy. Compressed Sensing (CS) has recently been introduced as a way to minimize the volume of data to transmit while still making it computationally safer to overcome the overlapping need for compression and privacy.
Symmetric and asymmetric lightweight IoT encryption algorithms are designed to achieve effective end-to-end communication by consuming minimal resources.

ETSI's Initiatives

In the upcoming years, ETSI (The European Telecommunication Standards Institute) will concentrate on Radio Equipment Directive (RED) and certification schemes to improve confidentiality and preserve customer privacy. To achieve these objectives, ETSI has considered activating the following articles under RED:

- Radio equipment does not harm or misuse network functioning and its resources.
- Radio equipment has protections to ensure that subscribers' personal data and privacy are secure.

Certain features that ensure fraud protection are supported by the radio encryption directive.

6.3 Authentication and Access Control

Introduction

Device authentication must get switched on as soon as the asset is added to the network, even before receiving data. Dedicated computer system devices need not wait for the user to provide a password to access the network. They need to be identified correctly before the authentication process occurs. The user authentication mechanisms will allow the user to know the network with username and password. These authentication mechanisms are referred to as Device-to-device (D2D) authentication. The other mechanism is a machine authentication mechanism that allows the device to access the network with the credentials stored in a secure storage area. Here the authentication credentials are exchanged through a Machine-to-machine (M2M) channel. The IoT devices encouraged lightweight approaches to maintain a sufficient performance transmission and improve the battery-operated devices' operating time. As a result, embedding a proper authentication protocol via circumspect design is critical from both a security and a transmission standpoint.

Access Control (AC) is the method of selective restriction of access to a place or other resource, while access management describes the process. Consuming, joining, or using are all words that can describe the process of accessing. Permission to access a resource is called authorization. Access control is the next step of authentication; there is no data security without authentication and access control. Access control assigns access privileges to various directory users and allows for the specification of appropriate credentials.

Authentication and access control are both step-by-step processes. Both authentication and access control must have high-security priority.

Research and Development

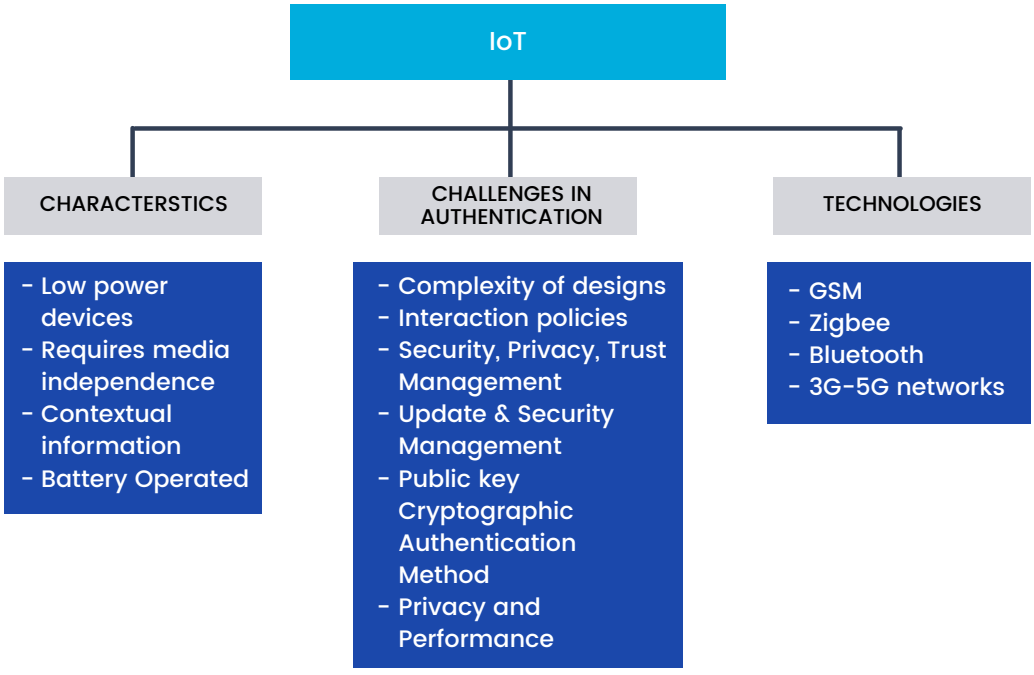


Figure 20. IoT R&D Overview

Cloud Database Compromise

The Cloud Database provides authentication, confidentiality, data secrecy, and other security properties like integrity, correctness, and availability. It is assumed that the attacker has read-only access to all the databases and the RAM of the physical machines. More or less, the attacker cannot modify the queries or the encrypted data but will be able to read and publish the sensitive data from the database. This threat is getting increasingly important in today's internet because of the flourishing of third-party clouds.

Low Resource and Low Power Devices

Low resource devices may lack the CPU and memory to perform the computation to encrypt and decrypt exchanged data. When a device essentially loses power, it can no longer function usually. This essentially constitutes a denial of service. An assault on machines with small energy reserves that causes their energy reserves to be used up prematurely is a common form of attack. For example, a common strategy to conserve power is for devices to enter various power-saving modes, e.g., various sleep and hibernation modes. A "sleep deprivation attack" is the most dangerous attack where the intruder prevents the device from entering its energy-saving mode. The victim nodes are bombarded with valid requests in a barrage attack. This threat is growing because these devices are increasing in today's world.

Updates and Security Management

Once the device is operational, it receives security patches and software updates. When rolling out security patches, the service provider or the device administrator must be authenticated by the device, such as that it does not consume bandwidth or should not compromise functionality or security. In the same way, as HMD global sends updates to their Android Mobile users, IoT products need software updates and security fixes, but their functional protection is compromised due to their restricted bandwidth and connectivity. These devices are dependent on security patches that are available to protect them against the vulnerabilities of the attackers. Keeping an eye on the future, as the number of devices grows, the speed of releasing updates will increase, and this needs active human intervention in the processing of the automated updates over the air. Exception activity will be handled and executed by automated human presence rather than handling and processing each update as soon as it arrives. If there is Human intervention in between the update process, then there are many chances of vulnerabilities.

Data Theft and Authentication

Health IoT, smart appliances, and similar devices collect a lot of data regarding their users. Users usually have no power over how this information is processed and distributed. In order to steal user data, an attacker may hack IoT devices.

Public-key Cryptographic Authentication Method

In an IoT device, there are two keys: a Public key and a Private key. A private key is impossible to get anywhere. But the public key is stored in the device. Technically, the real challenge is to initiate a secure connection between the Two IoT devices. This IoT device connection is called a Public key cryptographic authentication method. This method ensures the IoT device receives the public key that belongs to the intended communication channel and the peer IoT device is trusted. In reality, an IoT device may need to connect with various other IoT devices. It is tough to build robust security, as the hardware and the software differences between the various devices make it hard to develop a solution that would apply in every case. To add to the problem, manufacturers and creators of IoT devices often skip developing a security solution for their products to save money.

Trusted Communication

Trust is important in communication. Many IoT gadgets send messages to the network without encryption. This is one of the most critical security issues the industry is facing. It is high time that all the companies ensure encryption of the highest level among their cloud services and devices. If an attacker notices any flaws in the encryption, authorization, and authentication, he can access the cloud data through some methods. It is tough to detect a DDoS attack before it is launched, and hence the IoT market requires more effective and efficient DoS detection solutions.

Vulnerability Scanning

Vulnerability testing examines a computer's or network's possible exploit points to identify security gaps. A vulnerability scan identifies and classifies flaws in devices, networks, and communications infrastructure and predicts and suggests robust countermeasures. Security attacks are aimed at identifying flaws in target devices based on their software version and open services. This data can be used to launch targeted attacks against specific hosts.

Challenges in IoT Authentication

In an IoT device, there are two keys: a Public key and a Private key. A Private key is impossible to get anywhere but from selected trusted parties. But the public key is stored in the device. Technically, the real challenge is to initiate a secure connection between two IoT devices. This IoT device connection uses a Public-key cryptographic authentication method. This method is to ensure that the Public key received by the IoT device belongs to the intended communication channel and the peer IoT device is trusted. In reality, an IoT device is meant to interconnect with various other IoT devices. It is tough to build strong security, as the hardware and the software differences between the various devices make it hard to come up with a solution that would apply in every case. Adding to this difficulty, manufacturers, and developers of IoT devices often do not develop a security solution for their product to reduce costs.

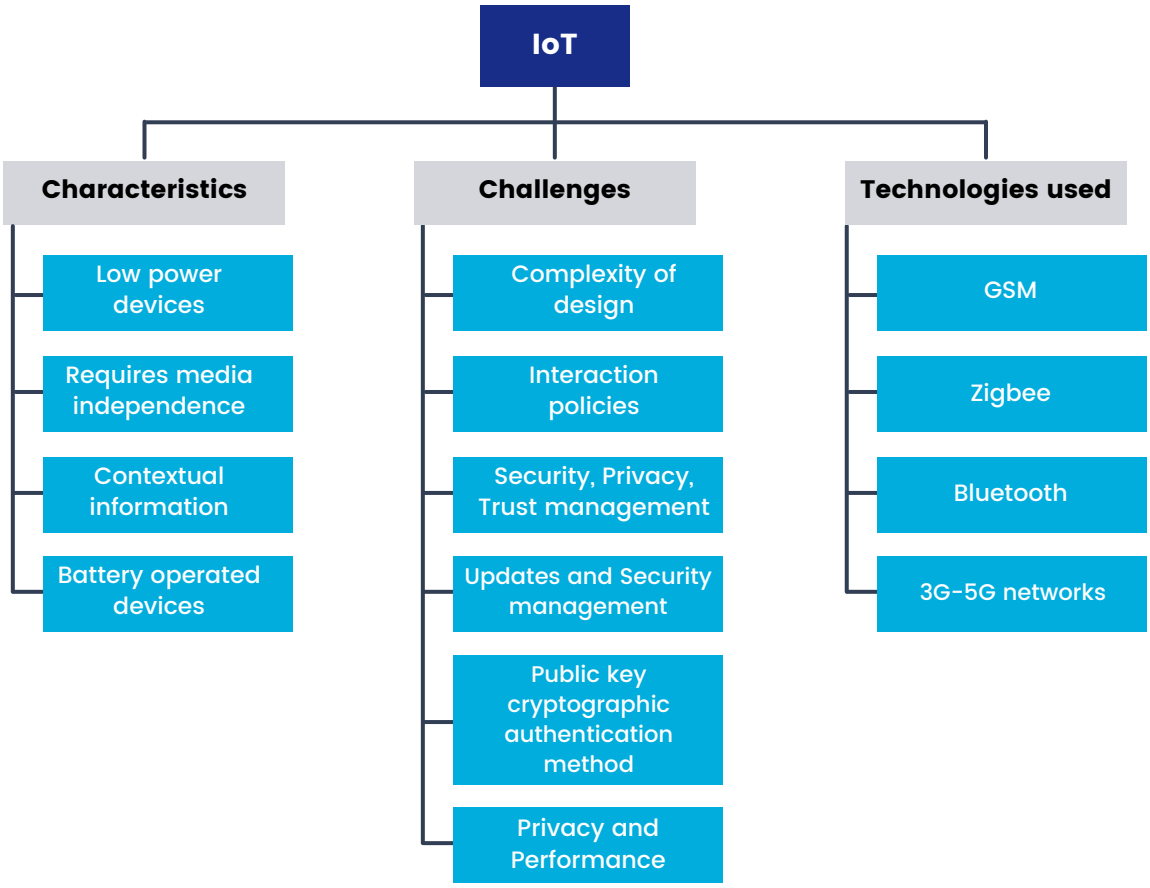


Figure 21. IoT Characteristics, Challenges and Technologies used

6.4 Identity Management

The importance of Identity and Access Management (IAM) in an Internet of Things system is supreme. IAM focuses on identifying individuals and controls their access to data (like sensitive data, non-sensitive data, or device data). IAM also assists with identifying computers and handling user access to files, thus preventing unauthorized access, data breaches and harmful practices.

Modifications to Suit IoT Systems

Current Identity and Access Management (IAM) solutions in IoT are limited in their ability to store identities and entities on a large scale. As a consequence of this restriction, there are no device integration layers for IoT-based applications. Hence, there is no proper method to discover and manage IoT identities. In a conventional IAM system, the standard approach provides restricted access based on an expected function rather than the least privileged access. As a result, authentication from the same device may provide different access capabilities based on the user role. IAM systems for IoT identity and access management systems need to include Machine-to-Machine (M2M) entities as well. The Regular IAM platforms will need to be updated or modified to suit the requirements of IoT systems.

M2M Communication

Machine-to-machine, or M2M communication, refers to any technology that allows networked computers to share data and execute activities without human intervention. The existing identity and access management systems provide secure, integrated data management from different devices and systems. Advanced security and trust management technologies, such as usage control, will, in the future, control autonomous data exchanges between various organizations.

Privacy Through Data Usage Control is an extension of traditional access control concepts. Future data usage control technologies will add labelling and tracking data similar to various systems processes to traditional concepts. Fine-granular usage restrictions will be defined to enforce privacy properties over large data sets while still running learning algorithms and analytics. The advantage of data usage control is that it allows users to control their data usage even when others manage it. It also meets the legal requirements in many jurisdictions (General Data Protection Regulation [GDPR] in the European Union).

Expectations in Upcoming IAM Solutions

The future IoT system implementations will need to control data exposure locally and interface with various other systems while maintaining end-to-end privacy guarantees. To be found in a series of related and heterogeneous devices, IoT devices use an Identity Management approach. Similarly, an IP address will identify a region in IoT, but each entity within that region has its unique address.

For the maintenance of the IoT security standards, first and foremost, the security features must be suitable for the device's design and purpose. In other words, the system should not be required to protect functions it lacks.

The following sub-sections outline standards in some key areas.

7.1 Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) translates to interconnected sensors, instruments, and other networked devices with industrial applications on computers, such as manufacturing and energy management.

IoT and IIoT principles are based on the availability, intelligence, and connectivity of devices. The only distinction between the two is how they are used in general. Although IoT is most widely associated with consumer applications, IIoT is used in manufacturing, supply chain monitoring, and management.

IIoT Standards

Several national committees and standards organizations are designing, prototyping, and fostering IIoT/smart manufacturing solutions standards. These organizations help businesses reach consensus and ensure the standards are freely accessible to those who choose to use them. There are various bodies like IEC, ANSI, and ETSI that provide leading standards.

For instance, B&R Industrial Automation uses the following standards:

- The Open Edge Connectivity includes Modbus and MQTT (Messaging Query Telemetry Transport).
- Ethernet, RS485.

IEEE standards are also used for IIoT applications in addition to these well-known ones. There are some internet standards also that some companies use, like ISA-95, which are also security standards.

IoXt: Internet of Secure things

The IoXt Alliance aims to increase consumer trust in Internet of Things products by establishing multi-stakeholder, regional, coordinated, and standardized security and privacy standards, product enforcement programs, and public disclosure of those requirements and programs.

The IoXt Security Pledge has eight simple rules:

1. The product should not have a default password; instead, it will require unique security credentials to operate.
2. The manufacturer is responsible for properly securing all product interfaces.
3. Product protection should be based on open, peer-reviewed methods and solid, validated, and updatable algorithms.
4. The manufacturer's default security settings for the product must be acceptable.
5. Only signed product would support software updates.
6. The manufacturer must act quickly to enforce security updates regularly.
7. The manufacturer must establish a vulnerability monitoring program to resolve challenges as soon as possible.
8. The vendor must be open about the length of time it would take to provide security updates.

Now, let us look into each of them in detail.

1. No universal passwords

One of the security flaws in connected devices is universal passwords. Very few people change their device's default password, making it easy for attackers to exchange password lists and gain access to people's homes. Every computer should, in theory, have a factory-programmed password that is exclusive to it. A sticker or QR code on the computer may be used to share this password with the user. When a sticker is not available or usable, the product can require a new password to be entered immediately after system installation. This password should, in theory, be complicated to guess.
The primary purpose of banning universal passwords is to prevent remote attackers from guessing a product's password, let alone controlling all units of a given system model. This means that each new computer would either come with its unique password or enable the user to create a password before the device can run. It is nearly impossible for a fresh-out-of-the-box device to be remotely breached.

2. Secured Interfaces

Linked devices can interact with one another to create product interactions in the home. Consider how your smart light bulbs interact with your remote control. Because of this interconnectivity, all sensitive interfaces that could be accessed and attacked remotely should be protected from breach, alteration, and monitoring. As a result, all product interfaces must be adequately protected. Not all devices are created or used in the same way because not all of them have the same attack surface.
At the very least, all devices must be protected against remote attack. Furthermore, some devices may be shielded from local attacks. Internal chip-to-chip interfaces may be protected in products where local attacks are a concern.

Stable boot or other memory integrity checks can also be used to secure the memory interface. Encryption and authentication are needed for all sensitive interfaces. This theory allows consumer product manufacturers to enforce “secure by design” measures to better protect a device against product interfaces given the device type and intended use.

3. Proven cryptography

Strong, established, updatable cryptography employing open, peer-reviewed methodologies and algorithms is required for product security.
Cryptography is a community-driven industry that requires freedom and community strength to flourish. Participants in the IoXt Security Pledge promise that their product's security will be based on verified and standardized cryptography. Wherever possible, appropriate cryptographic security approaches and algorithms that have been well researched, proven, evaluated, and standardized should be used instead of proprietary algorithms. Along with increasing interoperability and consumer choice, open standards are inherently safer than proprietary implementations because they not only offer their expertise, best practices, and work to the technology, but they also evaluate the security practices and test against vulnerabilities regularly. This enables open standards to be developed with security in mind and to develop swiftly, as well as to be resilient to emerging security threats.

4. Security by default

A consumer has a fair expectation that a new product would include adequate security protection. There is an option to turn off security in a device to download a third-party, potentially insecure app. Contrary to Apps from the authorized App Store, where applications are audited and protected. However, to begin with, there should be no requirements to make the system safe. One can enable higher levels of protection, such as preventing a child from making in-app transactions via their phone, just the way lower-than-default levels of security can be chosen. What is crucial is that there’s a standard level of protection that comes with the system. This theory ensures that goods are adequately protected when purchased. Although the customer can increase or decrease this degree of protection, the manufacturer would not leave the consumer unprotected by design.

5. Signed software updates

Only signed software updates should be supported by the product.
While all goods must be updatable, it's also important that these updated images be reliable. To prevent tampering during deployment, a manufacturer must cryptographically sign the updated images. Unsigned updates must not be used since they may be fraudulent. Injecting updated code into a device, on the other hand, poses a security risk because attackers may use this path to turn a device into some kind of bot. As a result, the manufacturer's updated images must be cryptographically signed. Furthermore, all updated images must be validated by the product before they can be used. Signed software updates safeguard all connected devices from remote attackers, which is a typical need and a necessity for all connected devices.

Secure boot defends against local attacks in which the adversary has physical access to the product. This principle assures that a device will only receive software upgrades that have been properly identified.

6. Automatically applied updates

The manufacturer will work swiftly to implement security upgrades as they become available. The manufacturer will automatically issue a fix to the product if a security vulnerability is discovered. There will be no need for user interaction.

Is it time to replace your security camera? That's a question no consumer should ever have to ask. To put it another way, a user shouldn't have to be the device's administrator. They shouldn't have to be a security specialist to make sure updates are installed correctly and swiftly.

Any upgrades or severe security flaws should be addressed without the need for user interaction. As a result, the manufacturer will automatically apply security patches as they become available. Because not all products can be distributed immediately, an update may be delayed slightly.

A connected car's brake system, for example, may only be updated after the vehicle is parked; doing any sooner may jeopardize driver safety. Alternatively, because many connected devices are spread across wide geographical locations, a manufacturer can opt to roll out a security update region by region to avoid peak data traffic on their networks. In other circumstances, products may be traveling through the supply chain and would be updated once they are linked to the web for the first time.

This approach assures that when consumers buy a connected product, it will be automatically protected and updated for the rest of its life, and these security upgrades will be implemented as quickly as feasible.

7. Vulnerability reporting program

The manufacturer must establish a vulnerability monitoring program to resolve challenges as soon as possible.

As part of a vulnerability disclosure policy, all companies offering internet-connected products and services must give a public point of contact for security researchers and others to report issues. Vulnerabilities should be addressed as soon as humanly possible.

When something wrong happens with a product or its services, who do you call a consumer— or even a researcher? Whom should you contact, and how can you be sure they've gotten your feedback and are taking action?

The device manufacturer or service provider must operate a vulnerability disclosure program that lets users, organizations, and researchers, to let them communicate their security concerns and even share new security techniques. An initiative like this will be established to allow newly discovered vulnerabilities to be responsibly disclosed and, if necessary, addressed quickly. Companies can use this principle to listen to their customers and industry developers. By providing a channel for direct communication and accountability, having a vulnerability reporting policy improves customer security care.

8. Security expiration date

Usually, consumers look for the manufacturer's warranty whenever they purchase a product. Similarly, consumers must make themselves aware of the warranty support period and the nature of security updates tied to the product when it comes to product security. Manufacturers shall ensure transparency about the warranty period of providing security updates. The duration of the manufacturer's security coverage will be clearly stated. Some companies may give extended security warranties to mitigate the continued engineering cost, while others may provide products with a lower warranty at lesser prices. The consumer has the choice to make an informed purchasing decision regardless of the model the manufacturer chooses. This avoids confusion among consumers about the course of security updates, thus allowing transparency about how long a device receives security support.

7.2 IoT Security Standards Protocols

IoT network protocols are used to link devices over a network. These are the communication protocols that are most commonly used on the internet. End-to-end communication protocol within the network's domain is possible with IoT network protocols. Let us look at the road to designing these protocols.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a non-regulatory body of the United States Department of Commerce specializing in physical sciences. Its purpose is to encourage industrial productivity and innovation. It was formed on March 3, 1901.

NIST for Cybersecurity

The Cybersecurity Framework is a set of guidelines for private sector businesses to adopt to be better equipped to find, detect, and react to cyber-attacks. It was developed by the National Institute of Standards and Technology, which is part of the US Commerce Department.
The challenge is aimed to promote device and data protection across business sectors and at scale in the Internet of Things (IoT) community. NIST is involved in a variety of IoT and IoT-related projects.

IoT work

Technical Needs

- Lightweight Encryption
- Advanced networking
- Cybersecurity for Cyber Physical System
- System BLE Bluetooth
- RFIF Security Guidelines
- Guide to Industrial Control System (ICS) Security

Specific Uses

- Connected Transportation
- Smart Cities
- Cybersecurity for Smart Grid System
- Wireless Medical Infusion Pumps

IoT-Related work

- Cybersecurity Framework
- Cybersecurity Framework profile for Manufacturing
- National Vulnerability Database
- Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- Digital Identity Guidelines
- Security Content Automation Protocol (SCAP) Standards and Guidelines
- Cyber Threat Information Sharing
- Supply Chain Risk Management
- Cloud security

Figure 22. NIST Involvement in IoT & IoT-related Projects

NIST organized an Internet of Things Colloquium, engaging participants from business, academia, and government to hear from the community to better understand the overall danger, protection, and privacy threat environment and what NIST can do to help these areas.

The following are the Cybersecurity and Privacy Risks of the Internet of Things (IoT).
Three high-level risk reduction priorities can be applied to cybersecurity and privacy threats for IoT devices:

1. Ensure the safety of your unit.

In other terms, prevent a system from being used to carry out attacks, such as eavesdropping on network traffic or breaching other devices on the same network. This objective applies to all IoT products.

2. Ensure the safety of data.

Protect data, including personally identifiable information (PII), obtained by, stored on, processed by, or transmitted to or from the IoT device's confidentiality, integrity, and/or availability. Except for those without any data that needs to be protected, this target applies to all IoT devices.

3. Ensure that individuals' data is protected.

Beyond the threats handled by computer and data security safeguards, protect individuals' privacy affected by PII processing. This target extends to all IoT devices that process personally identifiable information (PII) or directly or indirectly affect individuals.

Transducer Capabilities
This includes Sensing and Actuation

Interface Capabilities
This includes Human, Application and Network Interface

Supporting Capabilities
This includes cybersecurity and Privacy Capabilities

Figure 23. IoT Device Capabilities

The above figure depicts the IoT device capabilities. The following are some of the considerations for Cybersecurity and Privacy Risks:

Consideration 1:

Many Internet of Things (IoT) devices communicate with the real world in ways that traditional IT devices do not. IoT devices' interactions with the physical world can have several implications for cybersecurity and privacy.

Consideration 2:

Device Management, Monitoring, and Access Features. Many IoT devices are difficult to reach, control, or track in the same way the traditional IT devices are.

Consideration 3:

Capability in Cybersecurity and Privacy Availability, performance, and effectiveness are essential factors. IoT devices have different cybersecurity and privacy features than traditional IT devices regarding availability, performance, and effectiveness.

The following section explains the Proposals for Mitigating Cybersecurity and Privacy Threats:

Adjusting Organizational Policies and Processes

Organizations should ensure that their cybersecurity and privacy policies and processes resolve the issues that arise during the lifecycle of IoT devices. To prevent uncertainty and misunderstanding, organizations should clearly define their IoT scope. This is especially critical for companies that may be subject to laws and regulations that define IoT differently.
Organizations can also ensure that their cybersecurity, supply chain, and privacy risk management systems account for IoT. The following are examples of this:

1. Identifying which devices are capable of being connected to the internet of things: If it is not apparent, have processes to decide whether a product that is about to be procured or has already been procured is an IoT device.

2. Identifying the various forms of IoT devices: Understand the various types of IoT devices in use and the features and functions that each type supports.
3. Identifying the dangers of IoT devices: It's essential to understand the digital environment in which the IoT devices are deployed rather than assessing risks for IoT devices in isolation. Attaching an actuator to one physical system, for example, can have a somewhat different effect on risks than attaching the same actuator to another physical system.
4. Choosing whether to accept, refuse, mitigate, share, or transfer the risk by accepting, avoiding, limiting, sharing, or transferring it. All risk reduction techniques for traditional IT do not fit well for IoT.

Using Up-to-Date Risk Mitigation Techniques

An organization's cybersecurity and privacy risk mitigation practices require substantial changes because of the sheer number of IoT devices and the variety of IoT device types. Most companies have hundreds of traditional IT machines, such as desktops, tablets, servers, smartphones, switches, and firewalls. Traditional IT devices of the same kind usually have similar capabilities.

Most laptops, for example, have similar data storage and processing capacities, as well as human user interface and network interface capabilities, as well as supporting features like centralized management. With some customizations for specific devices and system models, organizations can decide how to handle risk for each of the hundreds of traditional IT device models.

The single-purpose design of most IoT devices enables most companies to have many types of IoT devices than traditional IT devices. With so many different types of IoT devices, organizations have to figure out how to handle risk.

Capabilities differ significantly between IoT system types. One lacks data storage and centralized control capabilities, and another has multiple sensors and actuators, utilizing the local and remote data storage and processing capabilities and being connected to multiple internal and external networks simultaneously.

Furthermore, an enterprise may need to decide how to handle risk not only by system type but also by device use. The intended usage of a system could mean that one security goal, such as honesty, is more critical than another, such as confidentiality, necessitating different risk mitigation mechanisms.

ENISA (European Union Agency for Cybersecurity)

ENISA (European Union Agency for Cybersecurity), founded on March 13, 2004, to contribute to EU cyber policy, improve the trustworthiness of ICT goods, infrastructure, and processes through cybersecurity certification schemes, collaborate with Member States and EU bodies, and assist Europe in dealing with daily cyber challenges.

Broad Attack Floor

The threats and risks associated with IoT devices and networks are numerous and rapidly evolving. Since IoT is heavily dependent on collecting, sharing, and processing vast volumes of data from several sources, including sensitive information and the fact that the data collection and processing are not always transparent to the users, these IoT devices pose an imminent risk and danger to citizens' health, safety, and privacy the threat landscape is changing.

There are significant technological and limited capabilities in an IoT device regarding computing, memory, and power. Hence implementing traditional security practices might be a challenge and will demand significant reengineering.
Security issues are compounded by the fact that IoT is associated with a rich, varied, and vast ecosystem encompassing aspects such as computers, communications, interfaces, and people rather than a set of individual devices.

Segregation of Rules and Requirements

The inconsistent and sluggish implementation of standards and regulations to direct IoT security measures and best practices and the constant proliferation of new technologies exacerbate related concerns.

Widespread Adoption

In addition to commercial IoT implementations, recent developments have seen Critical Infrastructures (CIs) transition to Smart Infrastructures by layering IoT on top of legacy infrastructures.
Due to potentially conflicting opinions and expectations from all interested stakeholders, security integration in these networks is difficult. Different authentication solutions, for example, can be used by different IoT devices and systems, which must be integrated and made interoperable.
Actuators operate in the real environment, and thus, safety concerns are very important in IoT. As the recent cybersecurity attacks on connected cars have shown, security threats can become safety challenges.

Reduced Cost

Because of the widespread adoption of IoT and the advanced functionalities it provides in various critical industries, there is potential for substantial cost savings by using features such as data flows, advanced tracking, and integration, to name a few. On the other hand, it is frequently the case that the low cost of IoT devices and systems has consequences regarding security.

Inadequate Technical Skillset

Since this is a relatively new domain, people are scarce with the necessary skillset and experience in IoT cybersecurity.

System Enhancements

Applying security updates to IoT devices is exceedingly difficult due to the user interfaces' unique nature, which precludes conventional update mechanisms. Securing such mechanisms is a difficult task in and of itself, particularly when considering Over-The-Air updates.

Unprotected Computing

Since IoT products face greater “time to market” pressure than other domains, attempts to improve security and privacy by design are constrained. As a result, IoT product developers prioritize functionality and usability over protection due to financial constraints.

In the event of a security incident, the lack of a clear assignment of liabilities may lead to ambiguities and conflicts, particularly given the broad and complex supply chain involved in IoT. Furthermore, the issue of how to handle protection if several parties share a single component remains unanswered. Another big concern is ensuring accountability.

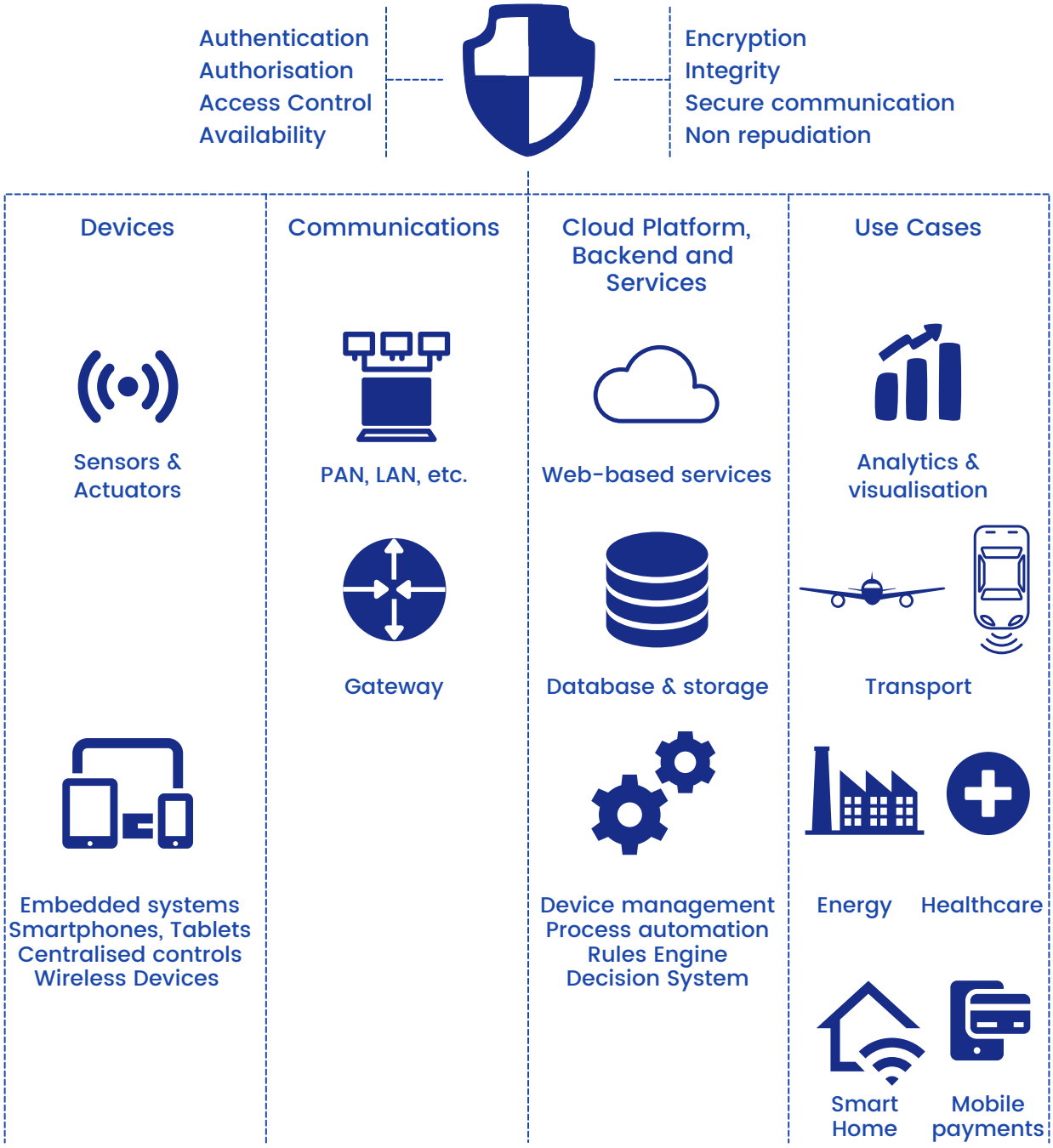


Figure 24. IoT High-level Reference Model

The image above shows the IoT high-level reference model. It's important to remember that we are not attempting to create a new IoT architecture or reference model. In contrast, by analyzing current such initiatives, we hope to abstract their fundamental elements to classify the properties to be covered consistently and systematically. Furthermore, in the sense of the IoT ecosystem, the horizontal aspect of protection should be emphasized. There are many security issues to consider, including authentication, availability, resilience, authorization processes, and the use of encryption to maintain data confidentiality both at rest and in transit.

The following are a few of the security precautions and best practices:

1. Security mechanisms for information system security risk identification, regulation, quality assurance, criteria and audit, and human resource security are included in information system security governance and risk management.
2. Ecosystem Management: This includes safeguards such as ecosystem mapping and relationships
3. Security mechanisms for system configuration, asset protection, system isolation, traffic filtering, and cryptography are all part of the IT Security Architecture.
4. Protection for administration accounts and administration information systems are included in IT security administration.
5. Security mechanisms for authentication, verification, and access rights are used in identity and access management.
6. Protection controls for IT security maintenance procedures and remote access are included in IT security maintenance.
7. Physical and environmental safety is also essential.
8. Security mechanisms for monitoring, tracking, and log correlation and analysis are all included in detection.
9. Security protocols for information system security incident investigation and response and incident reporting are included in computer security incident management.
10. Consistency of Operations: This section covers security measures for business continuity and disaster recovery.
11. Security measures for the crisis management agency and mechanisms are used in crisis management.

Categories

These security domains divide security measures into categories based on where they are used in an IoT ecosystem. Apart from their intended usage, each protection measure may be classified according to its nature: regulations that must be considered when designing products, organizational measures aimed at the company and employees that the organization must implement, etc.
As a result, the established IoT baseline protection measures are presented in three segments:

Policies

The first group of security initiatives consists of policies that are aimed at improving information security in general. These should be relevant for the activities of the organization and provide well-documented material. Following are some security best practices that have been established in this context.

Organizational, People and Process Management

Organizational criteria for information management must be in place in all companies. Their personnel practices must encourage good protection, ensure process management, and safely operate data in the organization's practices. Contractors and suppliers should be held responsible and accountable for the roles being considered.

1. End-of-life assistance
2. Relationships with third parties
3. Solutions with a track record
4. Risks and/or accidents in security are managed
5. Human Resource Management Security Policies and Training

Technical Measures

1. Management of trust and honesty
2. Security and privacy are strong defaults
3. Compliance and data protection
4. Security and dependability of the system
5. Guaranteed Updates to software/firmware
6. Authentication
7. Access control systems also protect physical and environmental protection
8. Cryptography
9. Communication that is safe and secure
10. Guaranteed networks and interfaces
11. Input and output security are also essential
12. Observation
13. Monitoring

Recommendations

Recommendations for Securing IoT at a High Level

ID	DESCRIPTION
1	Promote harmonization of IoT security initiatives and regulations
2	Raise awareness for the need for IoT cybersecurity
3	Define secure software/hardware development lifecycle guidelines for IoT
4	Achieve consensus for interoperability across the IoT ecosystem
5	Foster economic and administrative incentives for IoT security
6	Establishment of secure IoT products/service lifecycle management
7	Clarify liability among IoT stakeholders

Figure 25. Recommendations to enhance IoT protection at a high-level

Ensure that IoT Protection Initiatives and Guidelines are Consistent

There is a need to resolve the existing inconsistency of IoT protection protocols, initiatives, specifications, and other schemes. The definition of a list of best practices and recommendations for IoT protection and privacy, which can be used as a baseline for the implementation and deployment of IoT systems in the market, is a first and important step in the right direction (for example, reports from AIOTI and ECSO).
In terms of standardization, it is worth noting that the concept of standard is valued and accepted by the industry, but different groups of stakeholders have different R&D chains, which inherently leads to fragmentation. The recommendation is to define a collection of IoT practices, protocols, and security criteria consistent across Europe to combat fragmentation.
The Commission should facilitate this process, and the ENISA report should serve as a starting point for related efforts. Following that, each sector should develop its own set of practices, guidelines, and criteria for its own needs, based on the unique context and risk factors that each sector entails.

Exercise Influence On the Importance of IoT Safety

Cybersecurity is a disadvantage and is a cost for all parties concerned. As a result, it is critical that these stakeholders have a clear understanding of the risks and challenges they face and how to safeguard and defend themselves. Raising awareness is therefore important, and efforts to do so are strongly encouraged.

- Industry-wide security education and training are required, including state-of-the-art expertise, best practices, reference architectures, and the availability of building blocks, methodologies, and resources for stable IoT systems.
- To make informed decisions when purchasing IoT devices and systems, end-users and consumers must be trained. Campaigns to raise awareness about IoT protection are therefore critical, not only to maintain a basic level of cyber hygiene for the security of the “Things” that they have purchased or are running but also to maintain a basic level of cyber hygiene for the security of the “Things” that they have purchased or are operating.
- The developer community needs to be more mindful of the importance of adopting cross-vertical security standards rather than being bound to a single industry. Corporate IoT protection training is also useful and should be sought.

Establish IoT Hardware/Software Development Lifecycle Guidelines and make sure they are Stable

IoT product and solution developers, suppliers, and providers should integrate and adopt a stable Software Development Lifecycle (SSDLC) for their offerings and incorporate related processes into their operations. Security must be applied analytically, at the application stage, and in the SDLC.
By default, and security and privacy by design, security and privacy are natural foundation cornerstones of IoT security. Applying these principles in various contexts, each with its own set of characteristics is difficult.
The cyber risk in IoT is context-dependent (i.e., based on the use case), and protection and privacy by design criteria should be applied with this consideration in mind.

Adopting such values for the IoT environment can be aided by following relevant policies from other, more developed IT industries.
Safe-by-design hackathons and the use of best practice cookbooks for IoT protection will improve developers' perceptions of using security and privacy by default and by design principles. Developers may use the lessons learned from such activities to apply corresponding strategies to their projects and goods when it comes to businesses.

Obtain Interoperability Agreement throughout the IoT Ecosystem

Because of the IoT ecosystem's broad-scale penetration, long and complex supply chains, and various involved stakeholders, the topic of interoperability is extremely important. As a result, ensuring and encouraging interoperability of IoT devices, platforms, frameworks, and security practices is an important aspect of IoT security that should be encouraged.

The following are some suggestions that help in this direction:

1. Start encouraging the use of security-aware open interoperability systems.
2. Ensure that the security of interoperability systems is transparent.
3. Promote security interoperability labs and testbeds that are open and available.

Encourage IoT Protection by Financial and Administrative Benefits

Lack of protection affects business continuity, which is true even for IoT, fueled by R&D (Research & Development) and a hurry to get goods and services to market. In this regard, business continuity can be seen as a justification for investing in cybersecurity solutions.
Consequently, the market potential for cybersecurity is somewhat poor due to a lack of customer awareness of cybersecurity's added value. Consumer participation is important, and it should be encouraged further. Development planning campaigns should be introduced to increase and maintain said awareness, which would inevitably necessitate additional mechanisms. The competitive advantage is primarily based on time to market rather than security to the market for IoT. This balance should be shifted so that a certain degree of protection and privacy is encouraged before market deployment.

Set up a Stable IoT Product/Service Lifecycle Management System

Security is crucial over the entire lifecycle of an IoT product or service. Design, development, testing, manufacturing, deployment, maintenance, end-of-support, and end-of-life are examples of these phases (i.e., decommissioning). It is recommended that unique, focused, and security systems frameworks should be identified for all these steps.
Additionally, security procedures must be applied correctly. Fundamental security specifications and building blocks must be defined to be available within each process to achieve this.

Ensure that all the IoT Stakeholders are on the wage when it comes to the Liabilities

According to the expert interviews, one of the most critical issues to consider when considering IoT is a liability. It is especially crucial in the IoT domain since the cyber-physical nature of IoT connects and links protection and safety. It is necessary to resolve the issue of liability.

The issue of who bears responsibility for the IoT ecosystem's various stakeholders, such as developers, suppliers, providers, retailers, aftermarket support operators, third-party providers, and end-users, to name a few, is a complex one.

The questions of liability must be discussed in light of European and national regulations and case law; where holes in the law are found, they should be filled.

ETSI

The European Telecommunications Standards Institute (ETSI) is an autonomous, non-profit standardization organization in information and communications. ETSI is a non-profit organization that promotes developing and testing global technological standards for ICT-enabled systems, software, and services. It was founded in 1988.

IoT Standardization

Smart objects generate vast amounts of data. This information must be safely handled, interpreted, transferred, and stored. True interoperability between devices and applications requires widely agreed standards and protocols, which can only be achieved by standardization.

The application of standards:

1. Ensures cost-effective and interoperable solutions
2. Allows up a range of possibilities
3. Enables the industry to achieve its maximum potential

ETSI: Cybersecurity for Consumer IoT: Provisions

Consumer IoT

The Consumer Internet of things refers to the thousands of physical-digital devices now available, including smartphones, wearables, fashion products, and an increasing range of smart home appliances. All IoT system passwords have to be different and cannot be reset to a company reference value. Many IoT devices are sold with universal default usernames and passwords (such as “admin, admin”). This has been the cause of a slew of IoT security problems, and it is time to put an end to it. It is recommended to implement best practices when it comes to passwords and other authentication methods. The protection of a device can be further enhanced by providing a unique ID. As part of an approach that focuses on policy, companies that offer internet-connected products and services should provide a public point of contact for security researchers and others to report issues. Threats should be addressed as soon as possible.

As part of the product protection lifecycle, companies can continuously search for, detect, and correct security vulnerabilities in the goods and services they offer, manufacture, have made, and operate.

- All operating systems in consumer IoT devices ought to be upgradable in a safe manner. The responsible agency, such as the manufacturer or service provider, should notify the customer that an upgrade is needed. When software components are updateable, they should always be updated regularly.

- Inside services and on computers, credentials and data must be stored safely. Device programs with hard-coded passwords are not to be used. Hard-coded usernames and passwords in software can easily be discovered by reverse engineering of computers and applications. Users want products to fulfil their needs while still being resistant to encryption attacks. On the other hand, the appropriateness of security controls and encryption is determined by various variables, including the use of context.

- Close any software that is not in use and any network ports that are not in use. Hardware does not reveal access to assault unnecessarily (e.g., open serial access, ports, or test points). If software resources are not used, they should not be available. The functionality required for the service/device to work should be kept to a minimum. Software should be run with as little access as possible.

- Safe boot mechanisms, which call for a hardware root of confidence, should verify the software on IoT devices. The system should notify the user and/or the administrator if an unauthorized change to the program is detected. Also, it should not connect to any networks other than those used to perform the alerting feature.

- If an IoT system senses a problem with its program, it can notify the appropriate party. Devices can be set to administration mode in certain cases; for example, a thermostat in a room can be set to user mode, preventing other settings from being changed.

- Consumers must be given explicit and transparent details about how their data is used, by whom, and for what purposes by computer and service manufacturers and service providers. This includes advertisers and other third parties that may be involved.

- Where their use or other relying systems need it, resilience should be built into IoT devices and services, taking into account the risk of data network and power outages. In the event of a network outage, IoT networks should stay operational and locally available as far as possible and should restore cleanly in the event of a power outage.

- If telemetry data, such as utilization and measurement data, is obtained from IoT devices and services, these should be checked for security flaws. As telemetry data is obtained from IoT devices and utilities, personal data should be processed as little as possible and anonymized.

- Personal data can be conveniently deleted from devices and services when ownership is transferred, when the customer wishes to uninstall it, when the consumer wishes to withdraw service from the system, and/or when the consumer wishes to dispose of the device.

- IoT devices sometimes lose value and are recycled or discarded. Consumers should be given mechanisms that enable them to maintain control of their data removed from services, computers, and applications. When a customer requests that all their data must be deleted, they also expect the service provider to delete any backup copies they might have.

- IIoT system installation and maintenance should take just a few steps and adhere to security best practices for usability. Consumers should also be given instructions on how to set up their computers safely. By properly addressing ambiguity and bad design in user interfaces, security problems caused by customer frustration or misconfiguration can be minimized and removed. Validation is required for data input via user interfaces and data transmission via Application Programming Interfaces (APIs) or between network services and devices.

- Falsely formatted data or code transmitted through various types of interfaces may cause systems to malfunction. Attackers often use automated tools to exploit potential holes and vulnerabilities due to failure to validate data.

7.3 GSMA: Global System for Mobile Communications

The GSM Association (popularly referred to as "the GSMA" or "Global System for Mobile Communications, originally Groupe Special Mobile) is a trade association that represents mobile network operators around the world. The GSMA was established in 1995 as the 'GSM MoU Association' to assist and promote cellular network operators that use the GSM standard.

GSMA IoT Security Guidelines

IoT Service Ecosystems

The GSM Association (popularly referred to as "the GSMA" or "Global System for Mobile Communications, originally Groupe Special Mobile) is a trade association that represents mobile network operators around the world. The GSMA was established in 1995 as the 'GSM MoU Association' to assist and promote cellular network operators that use the GSM standard.

The Service Model

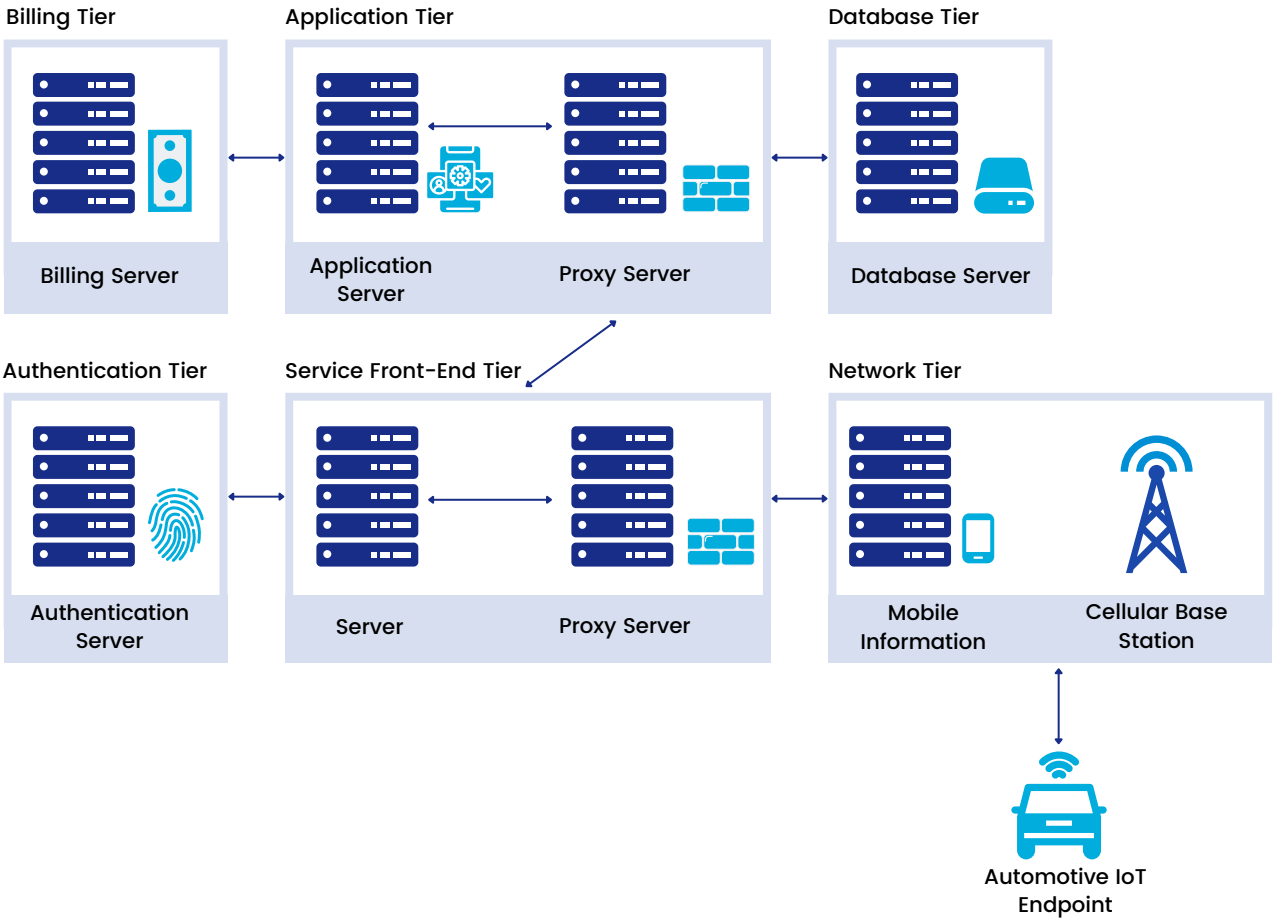


Figure 26. The Service Model

The Security Model

Regardless of the topology or technologies used to construct an application architecture, security in Service Endpoint environments can be built using standard infrastructure, techniques, and policies. The Service Ecosystem can be broken down into components to understand it better. Individually, these components must be protected but using similar methods.

Consider the components that create a simple service that can handle queries and send responses from end to endpoints, partners, and users. The following levels should be included in this model, but not confined to:

- A Web Service Tier
- An Application Server Tier
- A Database Tier, An Authentication Tier
- A Network Tier
- Third-party Application Tiers, such as a Billing Tier

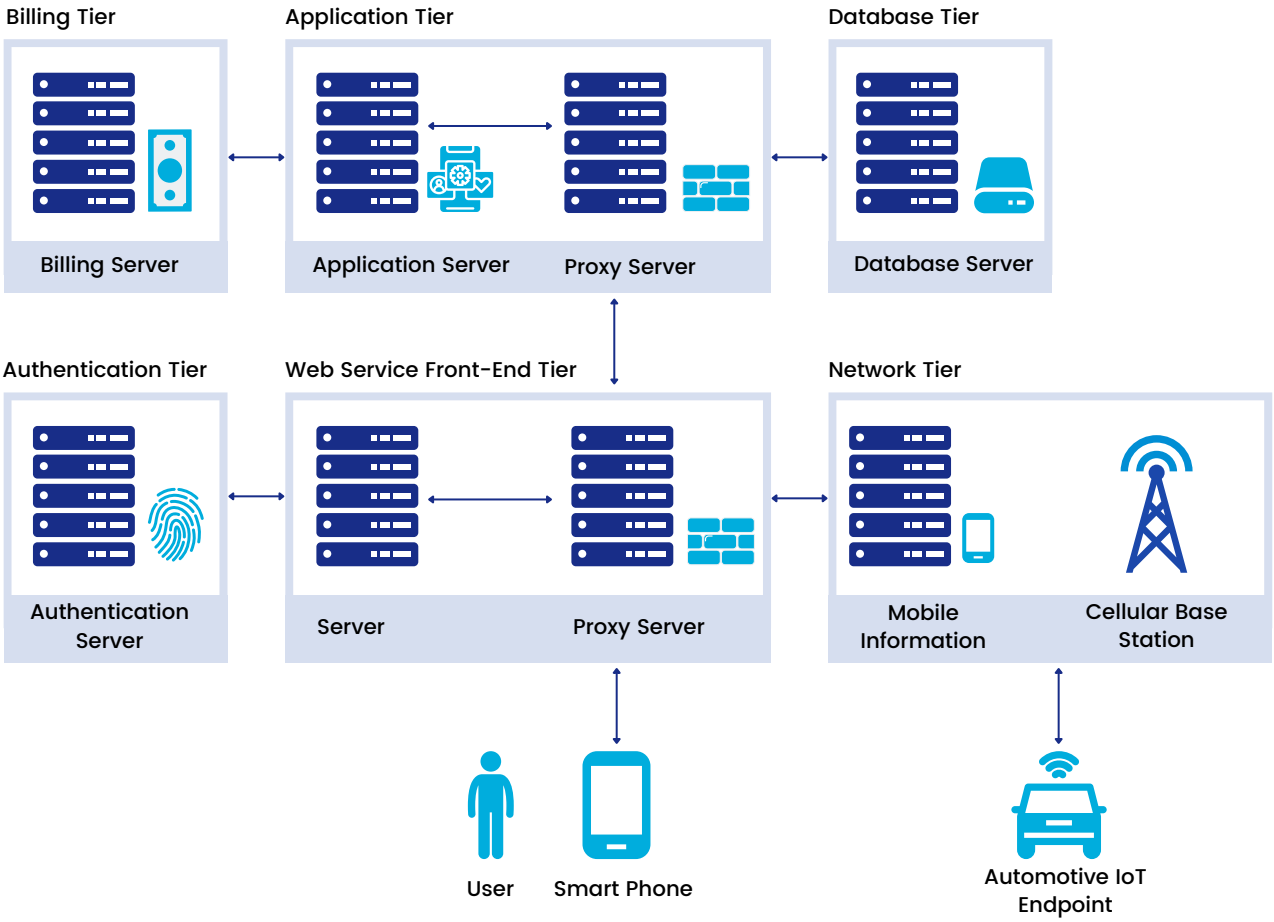


Figure 27. The Security Model

Network Infrastructure Attack

From a network perspective, attackers trying to penetrate the Service Endpoint would assume flaws in the way organizations interact and vulnerabilities in services exposed by service access points.

The Man-in-the-Middle (MITM) attack is the most common form of attack in this model. This attack assumes that the communications channel has no peer authentication, one-sided peer authentication, or broken shared authentication.

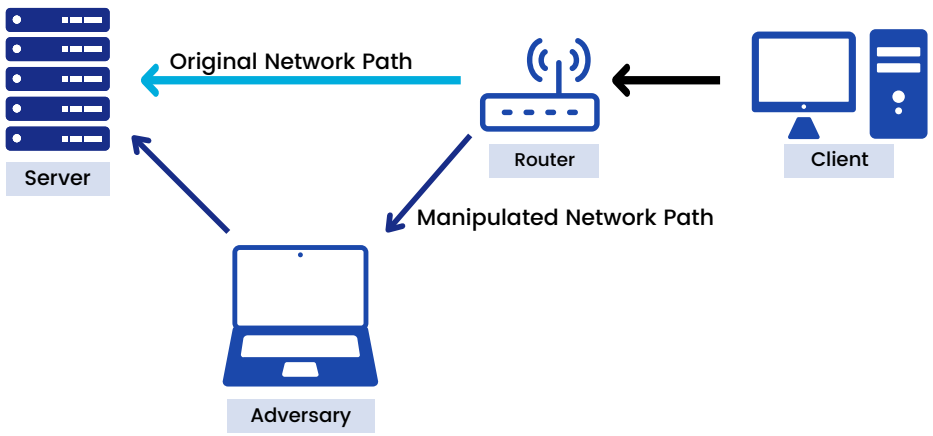


Figure 28. Network Infrastructure Attack

These attacks are difficult to carry out because they necessitate access to networking infrastructure within an organization, in the core Internet infrastructure between an organization and its partners or Endpoint Ecosystem, or near Endpoints.
Single endpoint attacks are limited to that endpoint or the community of endpoints accessible in that physical place. Border Gateway Protocol (BGP) hijacking, targeting a core router, or exploiting the Domain Name Service (DNS) infrastructure are common attacks against core internet infrastructure.
This model is simple to overcome using secure communication, forward secrecy, and suitable cryptographic protocols and algorithms, regardless of which form of attack is used.

Cloud or Container Infrastructure Attacks

These attacks need a privileged location on the Cloud or Container infrastructure. If an attacker can penetrate a Cloud service network, they can gain access to hosts running guest Virtual Machine (VM) systems.
Another Cloud or Container infrastructure attack assumes that the attacker controls a Virtual Machine (VM) on the same physical server as the target VM. The adversary may then use a variety of methods to attack other virtual machines on a physical server.

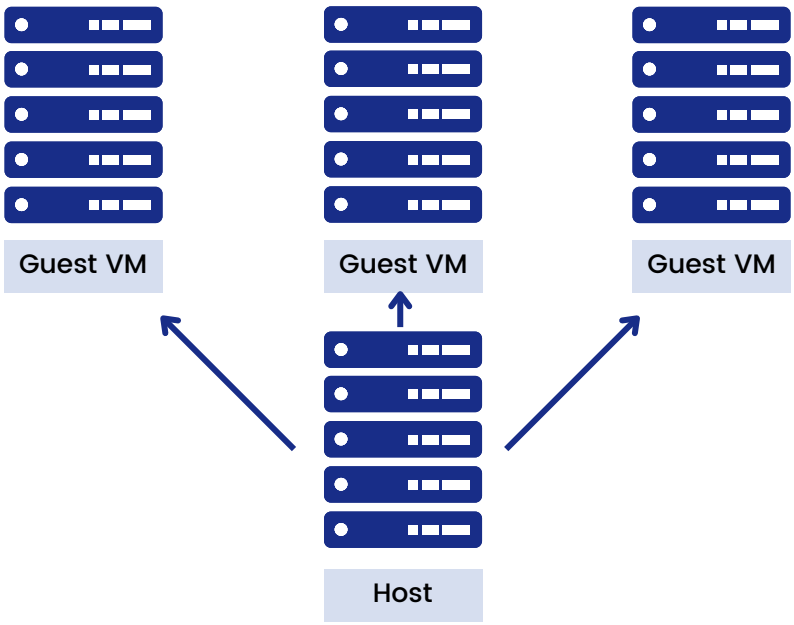


Figure 29. Cloud or Container Infrastructure Attack

Application Service Attack

Although discussions of application execution architecture are largely beyond the reach of this paper, it is important to remember that this layer is the most vulnerable to attack. Attackers can switch away from network infrastructure attacks to the application if the Service Ecosystem is configured correctly, as recommended in this document.
The application is the most complicated part of any product or service, and it always has the ability for an adversary to obtain power across several layers of technology.

Privacy

Although partner products are built to ingest data/metrics or other user-centric components to add value to the overall framework, the level of protection introduced by the partner can never be guaranteed. Rather than simply passing data to a third party, it is important to assess what types of information should be shared.

While contracts and insurance clauses can reduce legal responsibility, consumers can be lost due to a third party's failure. Rather than risking a business loss, a company can assess third-party engineering teams to see what degree of protection they employ in their infrastructure, software, and APIs.

Malicious Objects

Third-party systems are intended to provide customers with information, either plain or with multimedia. Advertising is one obvious way to do this. The structure of various types of files is complex, making it difficult for software to parse them correctly. Advertising networks are hence a facile medium for spreading malware.

Content Delivery Networks (CDNs) are also possible malware distribution channels. Malware can be transmitted by any device that provides complex multimedia types or bundles of code (web or executable) to render dynamic content.

As a result, the company must assess the various types of technical offerings distributed across a given channel. The company must determine what is acceptable and what is excessive to pass on to their customers.

For example, an advertising firm might want to send Java code to client systems via an IoT company's proxy service application. The company must determine if client systems operating in specific environments are more vulnerable to Java technology attacks. If this is verified, the company may decide to ban Java while allowing other technologies, such as Hypertext Mark-up Language (HTML), to pass.

There is no single standard way to ensure the end-protection users since malware comes in various ways, including polymorphous file types to Adobe Flash, Java, and multimedia exploits. An easy solution would be for the engineering team to impose a policy regarding which innovations should be used over their platforms and how they would affect their customers. Monitoring subsystems and sandboxes may be implemented to ensure that any object made on a client device is less vulnerable to abuse.

Authentication and Authorization

There are several great ways to share technology across networks. Engineers must ensure that technology does not unwittingly consume credentials that could be used to misuse permissions that were not explicitly given to a third-party service.

A few platform APIs allow restricting permissions to a class that the user either accepts or rejects. This helps the user to customize the experience to meet their unique privacy requirements. If the platform is unable to have granular security permissions, it can specify which technologies it needs.

The technical team must request that their partners permit granular permissions to ensure that revocation of a service does not unintentionally allow a window of disclosure of that user's data to resume even after the subscription is discontinued.

False Positives and False Negatives

Although monitoring and logging systems are excellent ways to supplement an established security system, they must be thoroughly scrutinized for false positives and negatives since these systems only interpret data from different ecosystems within an IoT product or service and are not created by the technical department.
However, they may not be able to tell whether an adversarial incident is taking place. Consequently, the IT and engineering teams must see if a suspicious incident is, in fact, the result of malicious activity. This would reduce the chance that the control team will deny a legitimate user access to the system.
Engineers must also be vigilant when modelling data acquired through analogue channels. False positives and false negatives may have serious implications if the application fails to adequately determine the best course of action if the acquired data cannot be completely trusted. This is particularly true in ecosystems where data must be processed at extremely high rates.

7.4 one M2M & IoT

The organization's mission is to establish a global technological standard for interoperability for Machine-to-machine and IoT technologies based on criteria submitted by its members.
In the IoT environment, oneM2M technology is eliminating fragmentation. It is a long-term solution for IoT implementation because it is independent of the connectivity- or protocol technologies used for transport.

The oneM2M architecture describes an IoT Service Layer, a vendor-neutral software Middleware that sits between processing and communication hardware and IoT applications and provides a collection of functions typically required by IoT applications. The oneM2M Service Layer provides case-independent functions.

CSFs (Common Service Layer Functions) from oneM2M include the following:

- User and application awareness
- User and program authentication and authorization
- End-to-end data security
- Remote provisioning and service activation
- Device management
- Connectivity setup and data transfer scheduling

The functions mentioned above are provided by the oneM2M common service layer, are exposed, and regulated by IoT applications through globally standardized vendor-independent and uniform APIs.

8.1 Introduction

5G is coming to connect all the citizens virtually through machines, objects, and devices. This upcoming technology aims to ensure that this medium delivers high speed of data, less latency, more reliability, increased availability, and provides an enhanced experience for the users. The fast and efficient performances will help to connect with the new industries.

8.2 Features of 5G

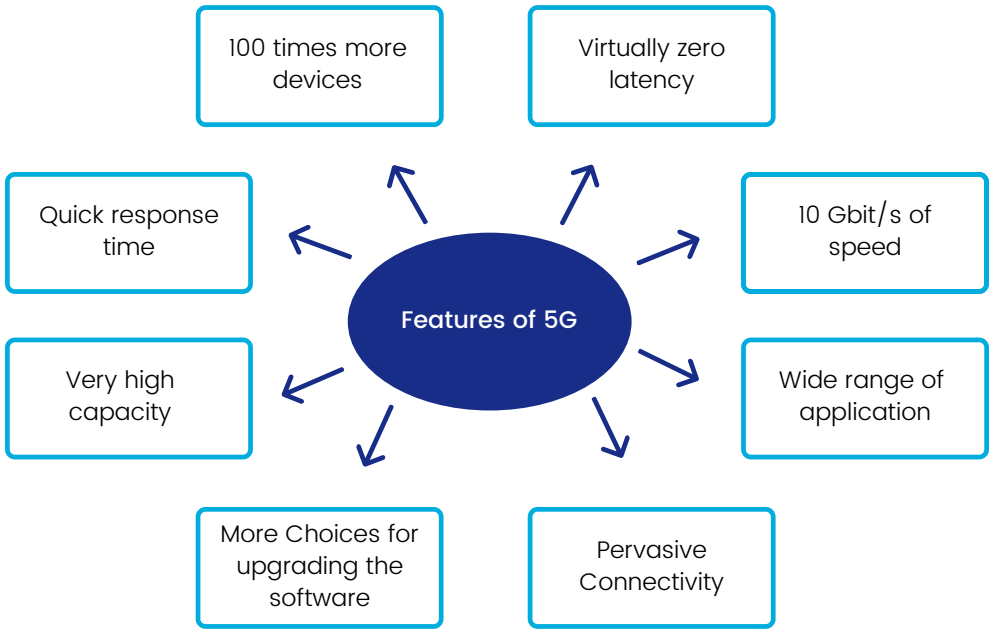


Figure 30. 5G Features

The features and their usage are way behind what human beings think. With vast speed, it is sufficient to change the definition of mobile phone usability. With advanced features, our smartphones will be parallel to the laptop. We can use broadband internet facility, wider multimedia options, connectivity, and high-quality sound, and HD videos can be sent through another phone with no trade-off. This will help the government to conduct any advanced courses and to supply the materials online.

8.3 Technologies used in 5G

5G network is based on OFDM (Orthogonal frequency-division multiplexing), which modulates different signals across various channels to minimise interference. The 5G OFDM works in the same way as the 4G LTE (Long term evolution) does. OFDM is the process of encoding digital information on multiple carrier frequencies. Moreover, the new 5G NR air interface will increase the strength of OFDM so that it can provide a high degree of flexibility. In this way, many people can access 5G for different use cases.
5G will bring wider bandwidths by expanding spectrum resources from 3 GHz used for 4G-LTE to 100 GHz and beyond. 5G can be operated in both lower bands (sub-6 GHz) and mm Wave (24GHz and up) which will help in bringing extreme capacity. 5G is deployed to deliver faster and supports expanding into new services such as mission-critical communications and connecting IoT.

8.4 Deployment of 5G

Beyond mobile operators, 5G is used for private networks with applications in Industrial IoT, enterprise networking, and critical communications. The 5G NR is launched depending upon the 4G LTE infrastructures pairing before ripening with the 5G core network. In the past two years, there is an association that stated that in 88 countries, 224 operators that have demonstrated, are training or testing, or have the license to conduct trials on 5G technologies are developing 5G technologies, or that they have announced the launch of 5G services. The first country to do so is South Korea in April.
When they launched this service, brands like Samsung, Ericsson, and Nokia have used carriers except LGU Plus. Among all the brands mentioned above, Samsung is the one who has launched the highest supply of 5G in South Korea by shipping 53000 base stations out of 86000 base stations implemented. Apart from these, there are other countries as well in which 5G radio hardware and 5G systems are implemented/used. Those are Altiostar, Cisco, Fiberhome, Huawei, Qualcomm, and ZTE.

8.5 5G Devices

In the 5G IoT chipset, there are four commercial chipsets and one commercial platform, with more launches coming soon. In March 2020, the first 5G smartphone was released. Due to its more advanced features, it is very expensive. In the US, it is around 1000 dollars compared to the Samsung Galaxy s10, which is about 750 dollars. In the same month, the Nokia company introduced the Nokia 8.3 5G, which claims that it has a wide range of 5G compatibility than other phones released. And in October, Apple introduced their first-ever 5G connected iPhone 12 and iPhone 12 pro.

8.6 Frequencies of 5G

The new frequencies are defined for 5G devices. The specification is divided into two frequency bands, FR1 (below 6GHz) and FR2 (mm Wave).
Frequency range 1 (< 6GHz): The maximum channel bandwidth given to FR1 is 100 MHz due to its scarcity of continuous spectrum in this crowded frequency range. The range of the band is 3.3-4.2 GHz.

Frequency range 2 (>24GHz): The minimum channel given to FR2 is 50 GHz, and the maximum is 400 GHz, with two-channel aggregation supported in 3GPP release 15. The higher the frequency, the greater will be the data-transfer speed.

8.7 5G and IoT

For IoT devices, having 5G is essential as it will help us in having the large capacity for a fast-working network to serve the connectivity. It will expand the frequencies that can transform the cellular data digitally. The wider 5G spectrum will increase the overall bandwidth for additional devices to connect. The 5G with IoT will also enhance in other fields which are Augmented Reality and Virtual Reality. The ultra-low latency will improve the AR/VR experience and open possibilities in businesses, education, etc.
This will not only enhance technological growth but also supports 22 million jobs around the world. We can expect this job growth from transport digitisation, manufacturing, agriculture, and other industries as well. We can also include construction sites, mines, oil derricks etc. These will greatly benefit from ultra-fast data transmissions to the time-sensitive nature of their outcome.
5G can bring advancements in smart industries. Going deeply through, IoT with 5G can run analysis on instantaneous virtual traffic, improving security, public safety, and enabling remote surgery if possible.
5G will act as a base for the full potential of IoT. 5G devices will play a huge role in our lives and evolve communications in business and industrial environments. With 5G's entry, the operators have to work not only on evolving the network but also on adding new opportunities to transform their businesses. Operators have achieved success in Phones, tablets, and computers; now, they have to implement innovative models to connect cars, meters, machine sensors, and consumer electronics. Today, most of the IoT revenues come from connectivity, but after five years, the revenue will also come from services, apps, and platforms.

Opportunities and Benefits for Enterprise

The enterprise segment will be the biggest source of the incremental 5G revenues for mobile operators. 5G will bring specific capabilities and flexibilities to provide services for customers from different enterprises. 5G cellular connections will bring more benefits than earlier 4G technologies. The difference between 4G and 5G will depend upon the latency. 5G can provide low latency which will be an advantage for manufacturing industries. In cities, 5G will play a major role in delivering an enhanced traffic management system by connecting traffic lights to IoT devices and sensors. 5G smart meters will help in reducing energy consumption.

5G and IoT Interconnection

- 5G is important as it can improve the range of IoT applications. Recent history states that 70% of the companies will spend around $1.2 billion on connectivity solutions. New businesses and start-ups need IoT devices with better performance criteria to provide security, low latency, wireless coverage and so on.

- In the coming stages, the LTE and 5G technologies will develop new connectivity interfaces for IoT applications. This technology will also bring Radio Access technologies (RAT), smart antennas, and making use of high frequencies by altering or re-altering the networks. The 5G enabled devices will help connect a large number of IoT devices to supply more wireless services in the market, which will boost rapid economic and social development.
- By using heterogeneous gadgets through consistent availability, IoT can alter and associate the global world. The idea of IoT has drawn consideration of the researchers to guarantee that wearables, sensors, clothes, watches, smartphones, tablets, etc are associated with a typical interface to interact with each other. The 5G mobile devices can guarantee those huge devices and new services, for example, enhanced multiple broadband (emBB), massive Machine-type Communications (mMTC), critical communications, and network operations are well upheld. It is believed that effective pre-requisites such as low latency, high versatility to empower a huge number of gadgets, etc., to clients will strengthen the utilization of the 5G system for IoT devices.
- Researchers stated that the future 5G mobile devices have to provide massive organization for IoT with billions of articles and sensors that will be a worldwide representation of the current scenario and help in the arrangement of basic utilisation of IoT cases that requires constant responses and automated dynamic procedures across various fields that include Vehicle-to-Infrastructure (V2I), high-speed motion, Vehicle-to-Vehicle (V2V), and process control system. In addition, there are some other upgrades presented in M2M and NB-IoT systems as described in the current 3GPP release-14 for cellular IoT, being the primary standards for 5G.
- The 3GPP standards are working to ensure that upgrades of KPI are installed into existing 4G systems, and also, the 5Gs should be developed from the very beginning to limit the cost of the growing new networks. For further advancement of IoT, it is suggested to create a context-aware congestion control (CACC) scheme for lightweight-based CoAP/UDP IoT network as a multi-target function that will speed up the exponential progress of the pattern of the conceived 5G networks for MTC application.
- The 5G portable broadband pre-requisites are not yet defined. The innovation, investigation, and advancements have just begun, and somewhere in the range of 5G can be accessed rapidly. In 2020, businesses can use the 5G devices, and IoT applications will be conveyed wherever with portable broadband innovation. Along with that, the big data produced by IoT applications will turn into a standard, and the cloud will be a great extent used to figure, store and virtualize arrange capabilities. The basic system foundation will embrace Software-defined Networking (SDN) to eliminate capital and operational cost.
- Four factors distinguish 5G connectivity from its predecessors. Those are:

  1. Connected devices
  2. Fast and intelligent networks
  3. Back-end services
  4. Extremely low latency

The factors mentioned above will help enable a connected and interactive world with many applications. That includes mobile broadband, AI, machine-to-machine communications, and advanced digital services.

- In the context of 5G device utilization in the healthcare industry, the connected people will help others to get quality care by improvement in treatment and diagnostics, and within a period, the businesses and consumers will have a strong bond with these devices. This will result in high-quality medical care in real-time and at an affordable cost. They expect to bring patients close to a Sci-fi concept of digital integration than ever before.
- For example, it is possible to transmit information to doctors through an electronic medium and based on that, the doctor will advise on diagnosis and treatment. It is the best method to reduce cost, and we can save time as well. There is no need to visit a doctor's office or hospital in case of a medical problem. Some routine visits can be attended at a distance, offering patients a greater alternative to conventional care.
- Sensors and monitors can also play a part in this. Remote devices will help patients based in isolated areas to access top medical assistance. Due to the current situation that the world is facing, video conferencing will be a great choice to bring high-quality health care to several under-served communities.

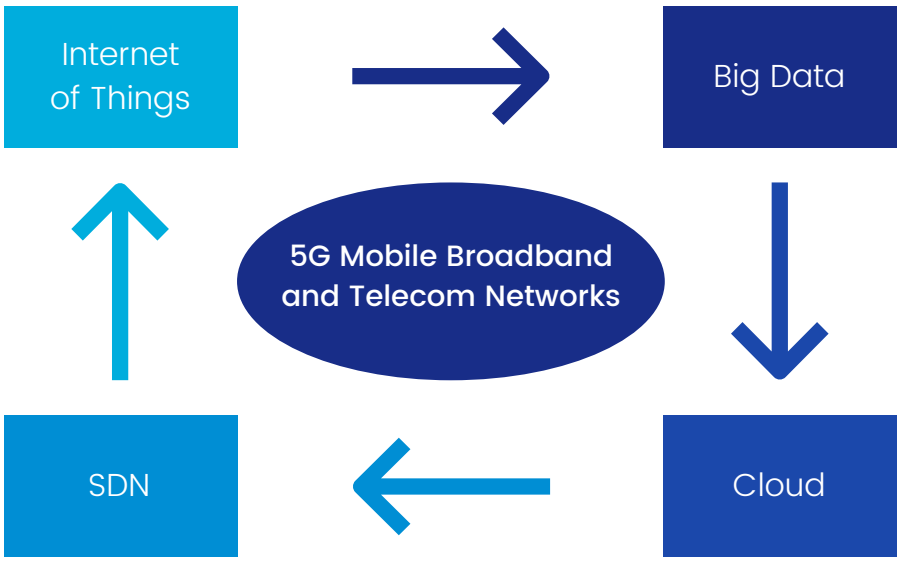


Figure 31. 5G Mobile Broadband & Telecom Networks

Based on the above figure, IoT will act as a gateway and transport network for IoT applications. Some of the technologies are listed to enable this interconnection between 5G and IoT.

1. Wi-Fi
2. Bluetooth
3. Zigbee
4. LoRaWAN
5. Z-Wave

The IoT is in high demand as the number of devices is increasing and will reach 3.2 billion in the year 2023.
Implementing a 5G network in it is one of the biggest news due to the following reasons:

Data-Transfer Speeds:

To boost any commercial sector, IoT plays a huge role, and with the 5G implementation, it will significantly increase the speed of data transfer. Based on the gathered data, 5G will work ten times faster than any other current LTE networks.

Greater Network Reliability:

In addition to its increase in speed, 5G networks provide more stable connections to work efficiently. A reliable and stable network connection is necessary for any IoT device, especially for locks, security cams, and other monitoring systems that rely on real-time updates.

IoT Testing Advice:

Discovering testing advice is good. It can help execute a better test result for the IoT projects to prepare well for the current and future IoT projects. To make a testing advance, two steps are required:

1. Expand Test Coverage:

IoT tests require extensive testing coverage. The ability of an IoT to work with a variety of new and old smartphones and tablets is crucial to its commercial viability. It's difficult to create an IoT that works effectively across a number of mobile operating systems and devices with varied hardware components due to fragmentation. As a result, it's critical to test on a variety of devices or configurations in order to detect issues caused by fragmentation.

2. Test From All Angles:

Secondly, to identify bugs that affect both the IoT device and its corresponding software (most likely a mobile app), testing must be conducted from various angles. Functionalities and usability must also be tested to gain an accurate report of connectivity quality (object to software, software to object, and behavior in case of interactions).

Test Bluetooth and Wi-Fi Connections:

The final step is to connect to or join the IoT to any mobile or other smart devices. First, check whether the IoT device can connect to other devices with the help of a Bluetooth connection and Wi-Fi networks.

Connected and remaining connected to an IoT device is difficult. If any bug occurs, it may cause problems while communicating and sharing data. To avoid this, it is essential to perform tests on IoT's ability to connect to other devices.

8.8 Security Recommendations for 5G

5G networks will bolster a host of critical functions, including smart electric grids, intelligent machines, and military communications. But it is very difficult to criticise 5G network infrastructure from a non-critical sort. As companies and individuals become more dependent on this network, they become more vulnerable to the theft of sensitive data traversing the network, attacks on the functioning devices that cause disruptions or the attack that degrades the network itself. 5G networks will expand the number and scale of potential vulnerabilities, incentives are increased for malicious actors to exploit these vulnerabilities, and making it difficult to detect malicious cyber activity.

One threat is the manipulation of equipment in the core network. For example, a piece of equipment is installed known as a "Backdoor" that allows interception and redirection of data or sabotage of critical systems. This occurs even if continuous tests are passed because the manufacturer will regularly send updates to the equipment. Such a threat can bypass front-end security measures such as inspecting source codes or equipment for backdoors and other vulnerabilities. Firstly, the core network functions will be in the cloud depending on the AI to manage complexity and network resource allocation. On such AI systems, hackers can get into these algorithms, and they can manipulate them accordingly.

On the edge, security is even more complicated. Backdoors are installed in the mobile base stations that will intercept or manipulate the data from one or more access points in the Radio Access Network (RAN). It won't be easy to trace such kind of activity. For example, if we copy the data, the base stations will operate normally only. The device that connects to 5G can itself pose cyber threats. In 2016, major internet activities were shut down as hackers hijacked low-cost chips in security cameras and digital video recorders (DVR) to take down multiple internet domains. The IoT architecture that is designed with web technologies increases the opportunities and consequences of such attacks.

The complexity of ensuring the 5G security and reliability requires a multi-layered strategy that consists of technical measures, regular adjustments, legal liability regime, diplomacy, research in investments, and cybersecurity skill training. From the technical point of view, networks require built-in resiliency that will help them isolate and withstand any single device's exploitation. They should have to use multiple vendors also if possible.

Regulatory policies should mainly focus on market incentives and transparency. The improved legal liability scheme is also necessary to improve private-sector cybersecurity. Such standards can exist with the other programs that will encourage the private sectors to share cyber-threat information with the federal government. The supply-chain risk management efforts are a key asset to it. Countries such as the US take some measures to protect their national information in 5G infrastructure. It should be available for innovation-driving investment to find out how they have made it a technology leader.

There are some strategies that we have to follow for a better 5G environment:

1. Meeting Consumers' Expectations

As the communication providers are switching to 5G, consumers' expectations are rising immensely. Analysis of 5G network experience has mainly focused on 5G speeds and availability by measuring the independent network measurements. In addition to that, we have to also see how the early adopters perceive the 5G network experience.

2. State of Consumer 5G

The demand for 5G is rapidly growing as the consumers now understand how much they are aware of the technology. But there is a large inconsistency across the globe in terms of knowledge and intention to upgrade 5G.

3. The 5G Knowledge Gap

Consumer awareness of 5G potential remains high. However, marketing technologies that are using high technologies now are somewhat lagging in understanding the value of 5G, device capabilities and offering. If the value of 5G technology has been better marketed, then the consumers who have already owned 5G-ready smartphones could have already got an upgraded 5G plan.

The service providers can adapt to it very quickly to provide a secure foundation. The initial 5G development started in the city centre, which was their main focus and the downtown areas required capacity augmentation and consumer perception. For example, in the UK, consumers have connected to the 5G network for around 1.5 times longer than those who stay in the suburban area. By improving the consumer perception, 5G availability will increase the likelihood by at least five times.

4. 5G needs more innovation

Consumers are highly satisfied with the 5G network performance, but they desire if 5G can give some innovative services for them. Some countries such as South Korea, Japan, China, and Taiwan are able to offer services for current 4G LTE networks, but at the same time, they are unable to implement them in 5G. They are still developing these services for 5G, which stops consumers from migrating to 5G.

8.9 Challenges in 5G

From a user perspective, privacy concerns centre around location tracking, identity, and other personal data. 4G has a larger network area since the signal is transmitted from a single cellular tower, 5G cellular networks have a small coverage area, and hence the signal strength is not good as 4G. When a user connects to a 5G network, the network can trace their location, and can even determine that the user is situated in which building. The threats such as using incorrect information to cause harm called security information attacks can find out the users' location. Whether the user is inside or outside, the 5G antennas can trace their location precisely.

With respect to identity, International Mobile Security Identifier (IMSI) attacks can reveal the identity of mobile subscribers. By grabbing the IMSI of the subscriber's device, the attacker can intercept the mobile traffic to monitor an individual's activity.

Even though the attacker can see the outgoing messages or calls, they still can not see what the message is about. After the individual leaves that attack, the attackers can still monitor past or future calls or messages.
Data collection is also one of the major issues for 5G users. Virtually all smartphone apps require personal information before or during installation. Application developers rarely describe where it is stored and what kind of data is going to be used. 5G does not contain any physical boundary and uses cloud-based data storage. The 5G users cannot protect or control their user data present in the cloud environment. Each country has its own data privacy policies, and this is seriously taken if and when the data is stored in the cloud of a different country.

8.10 Solutions for 5G

5G services should follow a privacy-by-design approach that is service-oriented and should preserve privacy. Mobile operators should follow a hybrid-based cloud approach where the sensitive information is stored locally, and less sensitive data is stored in the cloud. In this way, the operators can have access and control over their data, and they can decide where and with whom they want to share with.
Location-based privacy requires anonymity-based techniques where the user's true identity will be hidden. Before sending a message to a location-based provider, the message should be in an encrypted format. This will reduce the quality of the location, and it can protect the privacy of the location.
To prevent IMSI attacks, mobile operators can use Temporary Mobile Subscription Identity (TMSI). In TMSI, each mobile device is assigned to a random TMSI that is changed by the network at regular intervals. This will make the task difficult to identify mobile subscribers, and it will prevent them from getting eavesdropped on the radio interface.

8.11 Security Solutions for 5G with IoT

While 5G has been a conversational topic for many years, it is now becoming a global reality. Recently Verizon has expanded its 5G Ultra-Wideband services in various cities across the US. Samsung also announced that they introduced 5G devices, the Galaxy A51 5G and A71 5G. Soon, other Communication Service Providers (CSP) and smart manufacturers will follow this, and before we get to know, the 5G will completely disrupt connectivity, especially IoT connectivity. According to the Cisco report, by 2022, the 5G broadband (10 to 20 times faster than current 4G networks) will enable 12 billion mobile-ready devices and IoT connections compared to 9 billion in 2017. Combining higher bandwidth and low latency is a major challenge. It will indeed allow new use cases such as vehicle-to-vehicle and telemedicine; we should keep in mind that it can pose several security threats such as ransomware and botnet, among others. As the 5G network bandwidth and latency give rise to additional threat vectors within CSPs and hackers are getting more sophisticated in their attacks, real-time threat detection is vital. However, the current end-point security solutions that protect our devices such as smartphones and laptops fall short when it comes to securing IoT devices such as surveillance cameras and digital signatures.

For such cases, we have to implement network-based security solutions.
Virtualized 5G networks offer a platform for a range of new services that can be delivered through the network with no need for installation or upgrade from the subscriber. A security solution that works at a network level can compromise IoT attacks against malware and botnet attacks by performing behavioural analysis on the network traffic to identify and block the infections. Network-based solutions also perform remote remediation of suspect devices that block communications with bot command and control servers and other malicious servers. These network-based services can be provisioned and managed by the CSP to provide customers with an additional layer of in-line security for their IoT devices. CSPs can also enable services through a self-care portal through which communication behaviour analysis can be performed on a comprehensive IoT device. This portal will also provide traffic intelligence and control.
The increasing availability of IoT widely increases the threat landscape, and 5G will only further their security vulnerabilities as it powers new IoT devices. For that, the CSPs and customers must work together to protect their network plane to defend existing and new IoT connections from new and even more advanced attacks.

8.12 Ways customers can be prepared when prone to 5G security issues:

1. Use devices that are compliant with industry requirements:

Select IoT devices with built-in security features that satisfy NIST requirements and provide protection, detection, and mitigation.

2. Use a zero-trust policy:

Firewalls are no longer sufficient. Customers should adopt a zero-trust security approach. Nothing should be taken for granted. Everything, especially gadgets, should be double-checked.

3. Use virtualization to your advantage:

Customers can deploy security policies throughout their environment more rapidly with virtualized security controls, and automated remediation can help reduce attacks.

4. Take the help of a managed security service provider:

There is rapid innovation, complexity and change in 5G which results in rapid change and innovation in the security threats. Therefore, trust your Managed Security Service Provider (MSSP) to come up with new solutions.

5. Always have a security first mentality:

Always be alerted and report to security officials if you feel that anything is wrong. The objective is to manage the situation in such a way that harm is limited and recovery time and expenses are minimized. Therefore, learning about incident-response can be very helpful.

References

1. https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html
2. **What is a DDoS Attack? 2019, [online] Available:**
3. www.cloudflare.com/learning/ddos/what-is-a-ddos-attack
4. https://ieeexplore.ieee.org/document/9096818
5. **K. Sonar and H. Upadhyay, "A survey: DDOS attack on Internet of Things", International Journal of Engineering Research and Development, vol. 10, no. 11, pp. 58-63, 2014.**
6. https://www.cloudflare.com/en-in/learning/ddos/glossary/mirai-botnet/
7. https://success.trendmicro.com/solution/1118928-new-rapidly-growing-iot-botnet-reaper#collapseTwo
8. **M. E. Ahmed and H. Kim, "DDoS attack mitigation in Internet of Things using software defined networking", 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), 2017.**
9. https://www.researchgate.net/publication/335676455_IOT_Malware_An_Analysis_of_IOT_Device_Hijacking
10. **M.A. Crossman and H.Liu, "Two-factor authentication through near field communication," in 2016 IEEE Symposium on Technologies for Homeland security, HST 2016,2016.**
11. https://affinity-it-security.com/what-is-weak-authentication/
12. https://www.researchgate.net/publication/329140617_An_Overview_of_Potential_Authentication_Threats_and_Attacks_on_Internet_of_ThingsIoT_A_Focus_on_Smart_Home_Applications
13. **I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), pp.180-187, Larnaca, 2015.**
14. **K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," IEEE Wireless Communications, vol. 17, no. 5, 2010.**
15. https://www.logsign.com/blog/10-steps-to-prevent-man-in-the-middle-attacks/
16. https://www.kaspersky.com/resource-center/threats/ip-spoofing
17. https://www.acunetix.com/blog/articles/injection-attacks/

18. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” Ad hoc networks, vol. 1, no. 2, pp. 293–315, 2003.

19. W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, “A pairwise key predistribution scheme for wireless sensor networks,” ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 2, pp. 228–258, 2005

20. K. Sharma and M. Ghose, “Wireless sensor networks: An overview on its security threats,” IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs, pp. 42–45, 2010.

21. Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location-based compromise-tolerant security mechanisms for wireless sensor networks,” IEEE Journal on selected areas in communications, vol. 24, no. 2, pp. 247–260, 2006

22. https://www.acunetix.com/blog/articles/injection-attacks/

23. https://platform.keesingtechnologies.com/malware-attacks/

24. N. Provos, M. A. Rajab, and P. Mavrommatis, “Cybercrime 2.0: When the Cloud Turns Dark,” ACM Communications, Vol. 52, No. 4, pp. 42–47, 2009

25. Researchers Demo Cloud Security Issue With Amazon AWS Attack, October 2011.

26. https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/

27. https://portswigger.net/web-security/cross-site-scripting

28. CaoM,WangL,XuH,ChenD,LouC,ZhangN,ZhuY,QinZ. Sec-d2d: a secure and lightweight d2d communication system with multiple sensors. IEEE Access. 2019;7:33759–70.

29. Hao P, Wang X, Shen W. A collaborative PHY-aided tech- nique for end-to-end iot device authentication. IEEE Access. 2018;6:42279–93.

30. SN Computer Science (2020) 1:193 https://doi.org/10.1007/s42979-020-00201-3

31. Lin H, Bergmann N. Iot privacy and security challenges for smart home environments. Information. 2016;7(3):44.

32. Fernandes E, Paupore J, Rahmati A, Simionato D, Conti M, Prakash A. Flowfence: practical data protection for emerging IoT application frameworks. In: 25th {USENIX} security symposium ({USENIX} Security 16); 2016. p. 531–48.

33. R. Mortier, J. Zhao, J. Crowcroft, L. Wang, Q. Li, H. Haddadi, Y. Amar, A. Crabtree, J. Colley, T. Lodge, T. Brown, D. McAuley, and C. Greenhalgh, “Personal data management with the databox: What’s inside the box?” in Proceedings of the 2016 ACM Workshop on Cloud- Assisted Networking. ACM, 2016, pp. 49–54.

34. **Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot target- driven applications, Comput. Secur. 37 (2013) 111–123.**

35. https://vimeo.com/530802011

36. https://www.samsung.com/in/support/tv-audio-video/what-is-voice-recognition-feature-in-smart-tv/

37. https://ccm.net/faq/40606-samsung-smart-tv-how-to-enable-motion-control

38. https://mensgear.net/what-is-smart-tv-best-capabilities/

39. https://www.download.p4c.philips.com/files/5/55pfl8007k_12/55pfl8007k_12_dfu_eng.pdf

40. https://help.fitbit.com/manuals/manual_sense_en_US.pdf

41. https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793

42. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-a-virtual-firewall/

43. https://securityledger.com/2020/11/security-holes-opened-back-door-to-tcl-android-smart-tvs/

44. https://en.wikipedia.org/wiki/Smart_TV

45. https://www.welivesecurity.com/2018/10/01/protecting-your-smart-tv/

46. http://www.owlapps.net/owlapps_apps/articles?id=522938&lang=en

47. https://www.venafi.com/blog/traditional-cryptographic-attacks-what-history-can-teach-us

48. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8027141

49. https://fardapaper.ir/mohavaha/uploads/2019/06/Fardapaper-Current-research-on-Internet-of-Things-IoT-security-A-survey.pdf

50. https://vimeo.com/536329417

51. https://www.sailpoint.com/identity-library/7-best-practices-for-identity-access-management/

52. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard#:~:text=The%20Advanced%20Encryption%20Standard%20(AES,cybersecurity%20and%20electronic%20data%20protection.

53. **5G Security: Analysis of Threats and Solutions by Center for Industrial Information Technology (CENIIT), Ijaz Ahmad∗, Tanesh Kumar† , Madhusanka Liyanage‡ ,**

54. 5G Security: Forward Thinking Huawei White Paper by Huawei Technologies

55. 5G Security and Privacy – A Research Roadmap by Elisa Bertino, Syed Rafiul Hussain and Omar, National Science Foundation under Grant No. 1734706

56. Internet of things: Vision, applications and research challenges, Elsevier, Ad Hoc Networks by Daniele Miorandi a, ⇑, Sabrina Sicari b, Francesco De Pellegrini a, Imrich Chlamtac 2012

57. On Physical-Layer Identification of Wireless Devices, DOI by BORIS DANEV, DAVIDE ZANETTI, and SRDJAN CAPKUN 2012

58. On the features and challenges of security and privacy in distributed internet of things by Elsevier, Computer Networks, Rodrigo Roman a, ⇑, Jianying Zhou a, Javier Lopez b 2013

59. Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues by IEEE Communications Surveys & Tutorials, Jorge Granjal, Edmundo Monteiro and Jorge Sá Silva 2015

60. An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks, UTC from IEEE Xplore by Jing Zhang, Hong Zhong, Jie Cui, Yan Xu, and Lu Liu 2020

61. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges by IEEE Access, ANAM SAJID, HAIDER ABBAS, AND KASHIF SALEEM 2016

62. Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues, International Journal of Intelligent Computing Research (IJICR) by Hany F. Atlam, Robert J. Walters, Gary B. Wills

63. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks by NIST, Katie Boeckl Michael Fagan William Fisher Naomi Lefkovitz Katerina N. Megas Ellen Nadeau Danna Gabel O'Rourke Ben Piccarreta Karen Scarfone 2019

64. Security, Privacy and Trust for Smart Mobile Internet of Things (M-IoT), IEEE Access by VISHAL SHARMA, ILSUN YOU, KARL ANDERSSON, FRANCESCO PALMIERI, MUBASHIR HUSAIN REHMANI, AND JAEDEOK LIM6 2020

65. Security Protocols for IoT by, Research Gate by J. Cynthia, H. Parveen Sultana, M. N. Saroja and J. Senthil 2019

66. Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues by International Journal of Intelligent Computing Research (IJICR), Hany F. Atlam, Robert J. Walters, Gary B. Wills

67. Security Protocols for IoT, Research Gate by J. Cynthia, H. Parveen Sultana, M. N. Saroja and J. Senthil 2019

68. Internet of Things for Measuring Human Activities in Ambient Assisted Living and e-Health by Research Gate, Amine Rghioui, Sandra Sendra, Jaime Lloret, Abedlmajid Oumnad

69. On the features and challenges of security and privacy in distributed internet of things, Elsevier, Computer Networks by Rodrigo Roman a, ⇑, Jianying Zhou a, Javier Lopez b 2013

70. An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks, UTC from IEEE Xplore by Jing Zhang, Hong Zhong, Jie Cui, Yan Xu, and Lu Liu 2020

71. Security, Privacy and Trust for Smart Mobile Internet of Things (M-IoT), by IEEE Access, VISHAL SHARMA, ILSUN YOU, KARL ANDERSSON, FRANCESCO PALMIERI, MUBASHIR HUSAIN REHMANI, AND JAEDEOK LIM6 2020

72. https://platform.keesingtechnologies.com/malware-attacks/

73. N. Provos, M. A. Rajab, and P. Mavrommatis, "Cybercrime 2.0: When the Cloud Turns Dark," ACM Communications, Vol. 52, No. 4, pp. 42–47, 2009.

74. Researchers Demo Cloud Security Issue With Amazon AWS Attack, October 2011.

75. https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/

76. https://portswigger.net/web-security/cross-site-scripting

77. https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

78. https://searchsecurity.techtarget.com/definition/malware

79. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/smart-cities

80. https://www.businessinsider.com/iot-smart-city-technology#:~:text=Smart%20cities%20use%20IoT%20devices,utilities%20and%20services%2C%20and%20more

81. https://www.smartgrid.gov/the_smart_grid/smart_grid.html

82. https://www.digiteum.com/iot-smart-grid-technology/#:~:text=Smart%20grid%20IoT%20technology%20is,efficiency%20in%20the%20supply%20chain.&text=Adopt%20automated%20metering%20to%20monitor,maximize%20the%20use%20of%20renewables.

83. https://www.digi.com/blog/post/what-is-industrial-iot-definition-use-cases
84. https://www.acko.com/car-guide/connected-cars-features-benefits/
85. https://www.einfochips.com/blog/faqs-on-automotive-iot/
86. https://www.netguru.com/blog/smart-retail-solutions-that-change
87. https://www.lntinfotech.com/digital-transformation/internet-of-things/smart-supply-chain/
88. https://www.investopedia.com/terms/w/wearable-technology.asp
89. https://internetofthingsagenda.techtarget.com/definition/smart-farming
90. https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/

Abbreviations

AC	**Access Control**
AE	**Application Entity**
AES	**Advanced Encryption Standard**
AGA	**American Gas Association**
AIoT	**Artificial Intelligence of Things**
AP	**Access Point**
API	**Application programming interface**
APIs	**Application Programming Interfaces**
APTs	**Advanced Persistent Threats**
ARC	**Argonaut RISC Core**
BAN	**Body Area Network**
BGP	**Border Gateway Protocol**
BLE	**Bluetooth Low Energy**
CACC	**Context-Aware Congestion Control**
CAD	**Computer-Aided Design**
CAN	**Control Area Network**
CASB	**Cloud Access Security Brokers**
CDNs	**Content Delivery Networks**
C-ITS	**Cooperative Intelligent Transport Systems**
COAs	**Ciphertext Only Attacks**
CPCD	**Co-Processor Communication Daemon**
CPS	**Cyber-Physical Systems**
CS	**Compressed Sensing**
CSFs	**Common Service Layer Functions**
CSMA/CD	**Collision Detection**
CSP	**Communication Service Providers**
CSSP	**Control Systems Security Program**
CVSS	**Common Vulnerability Scoring System**
D2D	**Device to Device**
DCS	**Distributed Control Systems**
DDoS	**Distributed-Denial-of-Service**

DFD	Data Flow Diagram
DICE	Device Identifier Composition Engine
DLPs	Data Leak Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial-of-Service
DTLS	Datagram Transport Layer Security
DVR	Digital Video Recorders
E2E	End-to-End
ECSO	European Cyber Security Organization
EM	Electromagnetic Compatibility
EmBB	Enhanced Multiple Broadband
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FDE	Full-Disk Encryption
FOTA	Firmware Over-the-Air
FPGA	Field Programmable Gate Arrays
FR	Frequency range
GDPR	General Data Protection Regulation
GSM	Global System for Mobile
HG	Home Gateway
HMI	Human-Machine Interface
HMIS	Homeless Management Information System
HSCD	Hardware-Software Co-Design
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and access management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System

ICT	Information and Communications Technology
IDS	Intrusion Detection System
IMSI	International Mobile Security Identifier
IoT	Internet of Things
IoTSF	IoT Security Compliance Framework
IoXt	Internet of Secure things
IP	Internet Protocol
IRM	Information Right Management/Digital Rights Management
IV	Initialization Vector
KPAs	Known Plaintext Attacks
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
LINDDUN	Likability, Identifiability, Nonrepudiation, Detectability, Disclosure of Information, Unawareness, Noncompliance
LLC	Logical Link Control
LMP	Link Manager Protocol
LoRaWAN	Long Range Wide Area Network
LPC	Low Pin Count
LPWA	Low Power Wide Area Network
LPWAN	Low-Power Wireless Personal Area Networks
LTE	Long term evolution
LTTS	L&T Technology Services
M2M	Machine-to-Machine
MAC	Media Access Control
MTC	Machine Type Communication
MC	Mobile Computing
MDM	Mobile Device Management
MFT	Managed File Transfer
MITM	Man-in-the-Middle
MMTC	Massive Machine-Type Communications
MQTT	Messaging Query Telemetry Transport

MSSP	**Managed Security Service Provider**
NFMI	**Near Field Magnetic Induction**
NIST	**National Institute of Standards and Technology**
NR	**New Radio**
NSE	**Network Services Entity**
OFDM	**Orthogonal Frequency-Division Multiplexing**
OSI	**Open Systems Interconnection**
PaaS	**Platform as a Service**
PAN	**Personal Area Network**
PASTA	**Process for Attack Simulation and Threat Analysis**
PC	**Pervasive Computing**
PCB	**Printed Circuit Board**
PII	**Personally Identifiable Information**
PLC	**Programmable Logic Controller**
PnG	**Persona non Grata**
QR	**Quick Response**
R&D	**Research & Development**
RAM	**Random Access Memory**
RAN	**Radio Access Network**
RAT	**Radio Access technologies**
RBAC	**Role-Based Access Control or Conditional Access**
RED	**Radio Equipment Directive**
RTUs	**Remote Terminal Units**
RFID	**Radio Frequency Identification**
ROM	**Read-Only Memory**
RTOS	**Real-Time Operating System**
SaaS	**Software as a Service**
SCADA	**Supervisory Control and Data Acquisition**
SCAP	**Security Context Automation Protocol**
SDN	**Software-Defined Networking**
SED	**Self-Encrypting Device**
SoCs	**System on a Chip**

SQUARE	**Security Quality Requirements Engineering Method**
SDLC	**Software Development Life Cycle**
SSDLC	**Secure Software Development Life Cycle**
SSH	**Secure Shell**
TLC	**Technology Life Cycle**
TMSI	**Temporary Mobile Subscription Identity**
TPM	**Trusted Platform Module**
V2I	**Vehicle-to-Infrastructure**
V2V	**Vehicle-to-Vehicle**
VM	**Virtual Machine**
VPN	**Virtual Private Network**
WAN	**Wide Area Network**
WEP	**Wired Equivalent Privacy**
Wi-Fi	**Wireless Fidelity**
WLAN	**Wireless Local Area Network**
WPA	**Wi-Fi Protected Access**
WSN	**Wireless Sensor Networks**
ZT	**Zero Trust**
ZTA	**Zero Trust Architecture**