Foundations of IoT

Internet of Things 2

Mc Graw Hill

binarylogic

Foundations of IoT

Internet of Things 2

Foundations of IoT:
Internet of Things 2

Printed and distributed by McGraw Hill in association with Binary Logic SA.

Cover Credit: © ismagilov/123rf

MHID: 1265902860 ISBN: 9781265902865

mheducation.com **binarylogic.net**

Contents

1

IoT Advanced Applications

1

IoT Advanced Applications

INTRODUCTION

IoT technologies are transforming industries such as healthcare, agriculture, and city management by making them smarter, more efficient, and connected. This unit will explore how IoT applications are used in healthcare and agriculture, understand the architecture of smart cities, and learn about key technologies that enable secure data exchange and connectivity.

LEARNING OBJECTIVES

In this unit, you will:

- describe how IoT technologies are used in the Internet of Healthcare Things (IoHT).
- identify different smart healthcare applications.
- describe how IoT technologies can improve the agriculture sector.
- classify the oneM2M IoT architecture layers.
- clarify the functionality of the IoT World Forum architecture layers.
- identify the main characteristics of NFC and RFID technologies.
- define the technologies and the protocols that are used in Wireless Personal Area Networks (WPANS).
- identify the 5G network security challenges in IoT systems.
- describe the IoT privacy concerns and their possible solutions.

LESSON 1

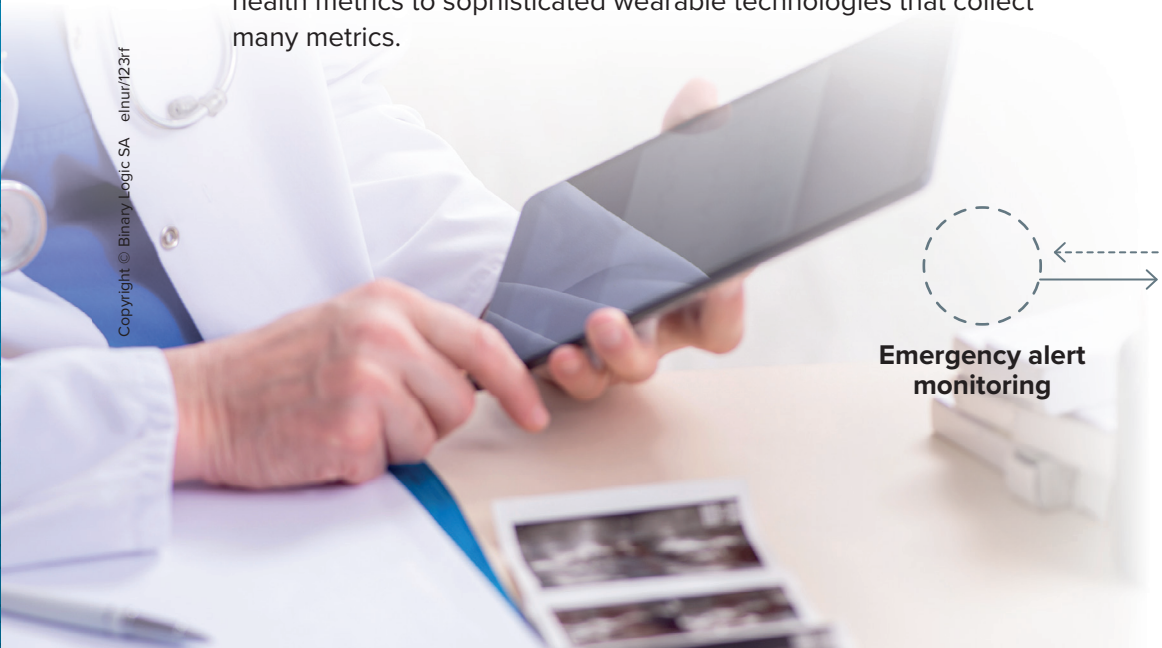
IoT Application Areas

Smart Healthcare

The implementation of IoT in the healthcare industry has a significant impact on society. IoT devices, such as wearable sensors, provide remote health monitoring, emergency alerts, and human well-being systems. In addition to monitoring health metrics, health-tracking gadgets include innovative wearable technologies that enhance the quality of life. From the observation of pediatric patients to the diagnosis and monitoring of chronic illnesses in the elderly, effective healthcare services can be provided for all ages.

The Evolution of Healthcare

The rapid population rise creates new challenges that can be solved with smart healthcare. Smart healthcare refers to the application of technology to improve the quality of life. Due to the absence of digital-era knowledge among healthcare workers, the transition to smart healthcare is slow. However, governments and private institutions are investing in the integration of technologies to improve the healthcare system. Traditionally, a patient would visit a doctor, a local medical center, or a hospital when needed. Smart healthcare helps patients to handle certain emergency circumstances independently. The focus on individual healthcare has shifted from traditional hospital treatment to smart home care. With the use of IoT devices, smart healthcare delivers remote health monitoring, emergency alerts, cost-effective treatment, and the availability of medical services regardless of location. These health monitoring devices range from fitness trackers that measure health metrics to sophisticated wearable technologies that collect many metrics.



Internet of Healthcare Things

The **Internet of Healthcare Things** (**IoHT**) is an IoT-based solution that uses IoT technologies to link people with various healthcare services. Specialized physicians can remotely review medical reports and records and provide recommendations without being in the same location as the patient. IoHT consists of networked medical imaging, lab reports, and remote healthcare monitoring devices. Medical imaging could be an X-ray, Magnetic Resonance Imaging (MRI) scan, Computerized Tomography (CT) scan, or other types of imaging. It also provides emergency services comparable to smart ambulances or smart clinics.

Wearables

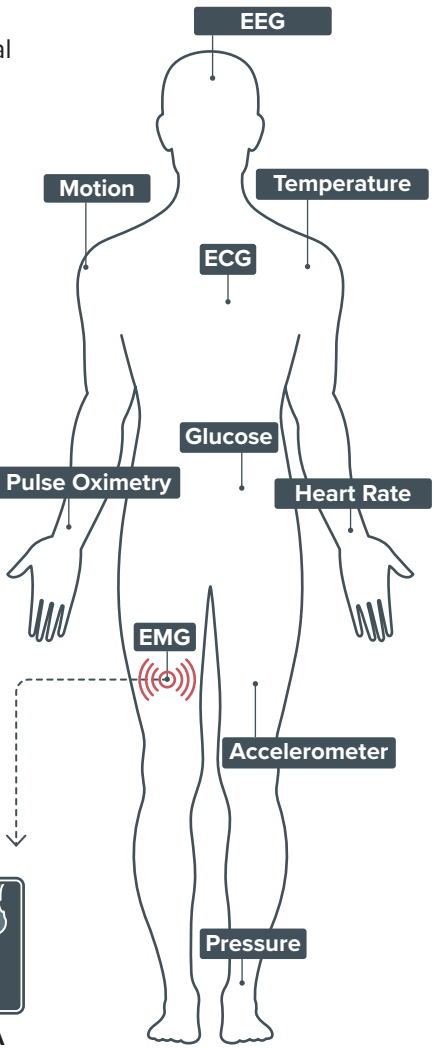
Wearables are smart objects placed on the human body. Wearable medical devices can gather, store, process, and analyze data to provide the required feedback and send alerts in emergency scenarios. The primary users are patients with temporary or permanent disabilities, the elderly, and babies. Biosensors on the patient's clothing capture data and produce a digital electrical output that can be utilized to monitor their health indicators. A biosensor is a small analytical instrument combined with a biological component to recognize events. Sensors and actuators differ based on the monitoring systems. They can collect and transmit data, such as bio-signals, body temperature, oxygen saturation level (Pulse Oximetry), movements, and geographic location. There are many bio-signals generated from the body, such as **Electrocardiogram** (ECG), **Electroencephalogram** (EEG), and **Electromyography** (EMG). Attached sensors can monitor physiological or biomechanical parameters, such as heart rate and muscle activity, respiration, body temperature, blood pressure, position, motion, and acceleration. The output of smart sensors and IoT devices is typically complex, necessitating the application of artificial intelligence, data analytics, and other technologies such as cloud computing.

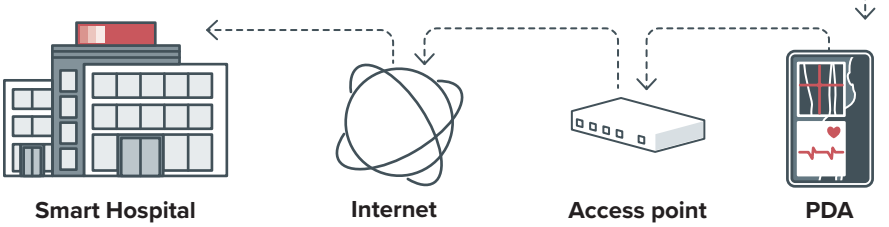
Electroencephalogram (EEG)

An electroencephalogram (EEG) is a diagnostic tool to identify brain electrical activity abnormalities.

Body sensor network

A **Body Sensor Network** (**BSN**) is a **Wireless Sensor Network** (**WSN**) used for human body monitoring. It is a wearable sensor node network that can communicate with other nodes and smart objects. These sensor nodes have computing, storage, wireless transmission, and sensing capabilities. For example, a blood flow sensor sends a patient's blood flow data to a smart device. This device is connected to the Internet and sends these data to the Smart Hospital. Even though BSN-based systems have a wide variety of applications, they can be used for continuous and non-invasive monitoring of vital signs, as tiny wireless sensors are placed on the skin and, in some cases, embedded in the clothing. This facilitates early disease identification and diagnosis. Typically, these sensors detect data on human body movement, body temperature, heart rate, skin conductance, and muscle functions.



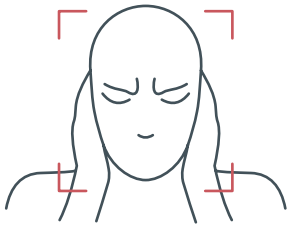


Smart healthcare applications

Blood pressure monitoring

Variations in the typical rate at which the heart pumps blood are associated with high blood pressure in humans. Hypertension, another term for high blood pressure, is a worldwide health issue caused by elevated blood pressure in the arteries. Chronic hypertension causes many problems, including heart failure, chronic renal disease, and blindness. Smartwatches are wearable IoT devices that, besides tracking a user's fitness and heart rate, can monitor other metrics like blood pressure and send the data for processing. IoT healthcare systems built on the cloud computing platform have become increasingly popular over time, allowing patients to monitor and control their blood pressure utilizing IoT devices.

Pain monitoring

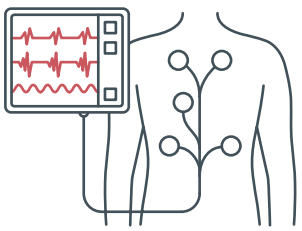


Identifying human emotions and pain is essential for delivering quality care to patients. Direct communication with patients or traditional means of interaction may not be adequate. Primarily children, the elderly, and those with mental illness require this form of engagement. Expressions on the face are a behavioral indicator of pain. Since the feeling of pain generates changes in facial expressions, they can be utilized as an automatic technique for diagnosing human discomfort. Instead of standard self-reporting methods, it can be used for people who cannot self-report, such as intensive care unit patients and infants. Infants' facial expressions are frequently observed by their parents because they convey information about their health. A solution is an automated pain recognition system that uses physiological inputs from IoT sensors and data analysis to evaluate different kinds of pain and emotions.

Electrocardiogram (ECG)

An electrocardiogram (ECG) is a test that measures the heart's electrical activity to determine whether the heart is functioning appropriately.

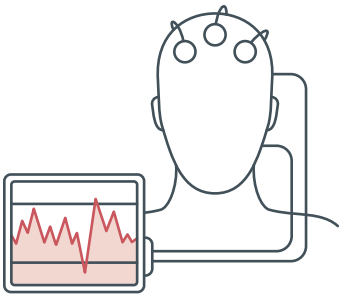
Electrocardiogram monitoring



Sensors on the skin capture electrical signals caused by heartbeats. Electrodes are typically positioned on the chest when an **ECG** is used in clinics. However, this setup is not suitable for everyday use at home. There are various smart objects for remote ECG examinations, and hospital doctors can process patient data from these wearable devices. Such an application can be built as a warning system to offer people cardiac health alerts and recommendations.

Sleep monitoring

Sleep is a natural and periodic state of mental and physical rest, but many individuals suffer from sleep disorders. There are various sleep disorders, including insomnia, sleep apnea, and obstructive sleep apnea. Obstructive Sleep Apnea (OSA) is a potentially fatal respiratory disease during sleep. It impairs quality of life by producing personality and behavioral issues. Countless systems are available for detecting OSA. One solution is wearable in-ear electroencephalography (ear-EEG) connected to the room's IoT network. This is a continuous and unobtrusive method of 24/7 sleep monitoring that assesses sleep quality. The captured data is used to predict the sleep stages utilizing Artificial Intelligence algorithms.



Pathology monitoring

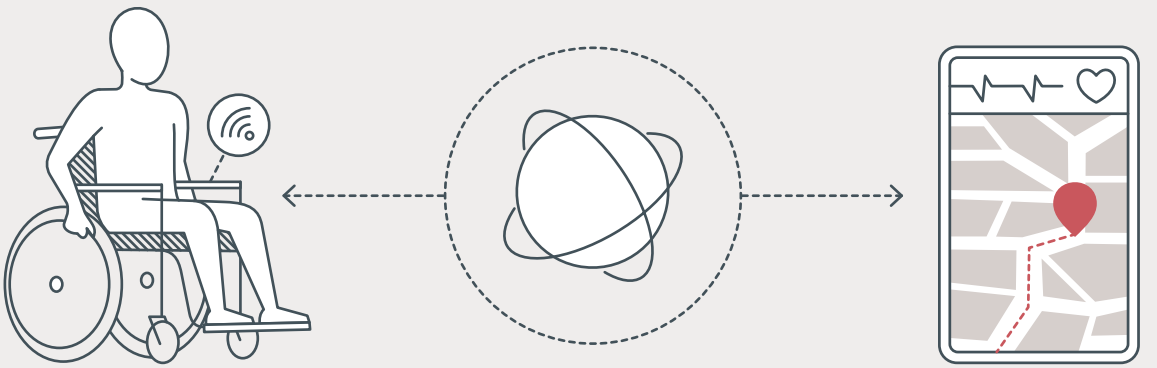
Pathology is the scientific study of the origins and effects of disease and injury. In an EEG, this is accomplished by attaching small metal disks with thin wires to the scalp which send signals to a computer to store the results. EEG is frequently employed for this purpose because of its low cost and non-invasive nature. EEG can diagnose some brain-related disorders, such as epilepsy and stroke. Patients with these conditions require immediate attention because any delay can be fatal. An IoT system that monitors the patient's condition can be life-saving in such situations.

Disabled persons monitoring

Smart wheelchairs (SMW) connected to IoT systems is a new research topic. The design of these systems consists of two elements: a mapping service used for navigation and a client wheelchair. SMWs incorporate 3D **LIDAR** for mapping their external environs and autonomous movement without Global Positioning System (GPS). This technology employs both a control architecture for the motorized wheelchair and an embedded system for monitoring critically ill patients. The embedded system also uses the user's biometric characteristics to detect potentially dangerous situations. The wheelchair would generate a warning by activating the alarm upon measuring the heartbeat and blood pressure spikes at a certain interval.

Light Detection And Ranging (LIDAR)

Light Detection And Ranging (LIDAR) is a technique for measuring distances by pointing a laser at an item or surface and measuring the time required for the reflected light to return to the sender.



Smart Agriculture

The agricultural sector can improve and optimize most workflows by utilizing many IoT technologies. The implementation of the IoT in today's agricultural sector has particular advantages, such as the efficient use of resources like land, water, fertilizers, and pesticides; an improvement in profitability, sustainability, food safety, and environmental protection; and a decrease in production costs.

Smart agriculture applications

Precision farming

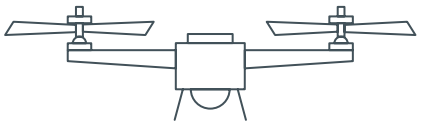
Precision farming refers to watering plants per their location and water amount requirements. This type of farming requires data from many sensors, such as plant location, humidity, and surface temperatures, which may be obtained largely by aerial monitoring.

Remote-controlled aircraft, often known as **Unmanned Aerial Vehicles** (**UAVs**) or drones, have gained popularity for aerial monitoring. Over the past years, UAVs have been utilized extensively for tracking cultivated fields and providing effective precision agriculture solutions. Using remote sensing, it is possible to follow a variety of crop and vegetation metrics using images of varying wavelengths. Historically, remote sensing relied heavily on satellite imagery. UAV systems have proven effective in various precision farming applications, including pesticide application, water deficit recognition, and disease identification. Numerous decisions can be made based on the data captured by the UAV for estimating yield in order to fix the identified problem and maximize production.

The role of UAVs is to capture data with precise spatial details. Many sensors are used depending on the agricultural parameters that must be monitored. UAV sensors must meet three essential requirements: low energy consumption, light weight, and small size. These techniques create environment maps that depict the soil morphology, allowing for more efficient irrigation planning for each crop. Global Positioning System (GPS) technologies are widely utilized to assist in the localization and georeferencing of objects captured by remote sensing. Since remote sensing information is a rich source of environmental data, it is usually imported into Geographic Information Systems (GISs) and combined with other datasets.

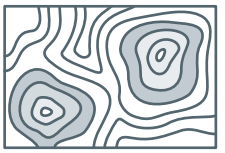
Unmanned Aerial Vehicle (UAV)

Unmanned Aerial Vehicles (UAVs) are aircrafts without human pilots, crew, or passengers.



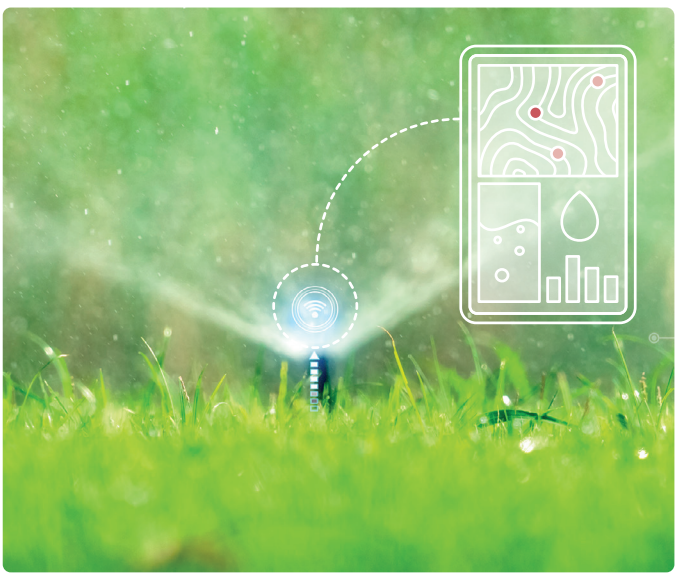
Low energy **Light weight** **Small size**

Important types of sensors used by UAVs

Sensor type	Description
 Visible Light Sensors	Visible light sensors can take images in various conditions, including sunny and cloudy weather. However, the quality of the photos depends on light conditions.
 Thermal Infrared Sensors	Thermal infrared sensors measure surface temperatures. Using infrared sensors and an optical lens, thermal cameras collect infrared energy. Thermal imaging cameras focus and detect radiation at the same wavelengths, transforming it into grayscale images representing heat. Multiple thermal imaging sensors can create a colored image.
 Multispectral Imaging Sensors	Multispectral imaging sensors collect visible wavelengths as well as wavelengths that fall outside the visible spectrum, including near-infrared radiation (NIR), short-wave infrared radiation (SWIR), and others. UAVs with multispectral or hyperspectral sensors collect crop absorption of water information. Despite their increased cost, spectral data can be quite valuable for evaluating many biological and physical characteristics of crops.

Precision irrigation

Precision irrigation is a micro-irrigation technique that conserves nutrients and optimizes water required by plants. It slowly provides plant roots with water droplets below or above the surface. Crop productivity is increased by adopting precision irrigation IoT technologies. The installed sensors identify or read the physical and chemical aspects of the farmland, including the weather, temperature, humidity, plant health, soil moisture, soil acidity, and soil nutrients. The collected data are analyzed to inform farmers of the necessary adjustments. Data analysis assists in determining the appropriate nutrients and their quantities, as well as the water needed for irrigation.



Vertical farming

Vertical farming is the cultivation of plants at a vertical scale, rather than horizontally. Only a small area is needed for a crop to thrive, and multiple types of crops can be cultivated concurrently. Using IoT technologies, devices may be remotely handled using communication technologies such as Bluetooth, Wi-Fi, and RFID.

Typically designed for urban environments, indoor vertical farming creates an ideal climate for crops without the impact of external environmental factors. IoT technologies play a crucial role in managing the farming environment, as well as monitoring plant health and watering needs.

Vertical farming also requires the processing and analysis of vast amounts of data for crops to develop effectively. With the help of technology, agricultural productivity can be optimized by automating the entire process, from seed to harvest, in a controlled environment.

EXERCISES

1 Choose the correct answer.

1. What is one of the primary capabilities of the Internet of Healthcare Things (IoHT)?

A. It enables patients to perform complex surgeries remotely.

B. It allows for real-time sports coaching across locations.

C. It provides remote review of medical records and recommendations by specialists.

D. It supports only the storage of patient data without analysis.

2. Which type of data can a Body Sensor Network (BSN) collect?

A. Environmental pollution levels

B. Geographic positioning data

C. Body movement, temperature, heart rate, and skin conductance

D. Audio and video recordings for telehealth sessions

3. What is the purpose of Precision Farming in Smart Agriculture?

A. To increase the use of pesticides.

B. To track plant health and optimize water and nutrient requirements.

C. To reduce the need for human labor exclusively.

D. To focus solely on increasing plant varieties.

2 Define what the Internet of Healthcare Things is.

3 Distinguish what data types can be collected by wearable smart objects.

4 Describe what a Body Sensor Network is comprised of.

5 Analyze how AI solutions can be used for IoHT solutions for pain monitoring.

6 Describe how UAVs are used for precision farming IoT solutions.

LESSON 2

IoT Networking Technologies

OneM2M Architecture Versus IoT World Forum Architecture

The rapid development of **Machine-to-Machine** (**M2M**) communications has resulted in the creation of IoT architectures. These architectures help accelerate the adoption of M2M applications and devices including the Internet of Things. The **oneM2M architecture** and the **IoT World Forum Architecture** are considered widely known IoT architectures. The oneM2M architecture designs IoT solutions with only the devices and their applications in mind. The IoT World Forum Architecture is used to design IoT applications while considering technologies such as data storage, data processing, network connectivity, and **edge computing**.

OneM2M architecture

Managing the variety of devices, software, and access methods is one of the biggest challenges when developing an IoT architecture. By creating a horizontal platform design, oneM2M architecture is building interoperability standards at all levels of the Internet of Things stack.

The oneM2M architecture organizes IoT functions into three layers: the application layer, the services layer, and the network layer. This architecture may seem relatively basic; however, it is very rich, encourages interoperability via IT-friendly APIs, and supports a vast array of IoT technologies.

Application layer

The oneM2M architecture prioritizes connections between devices and their respective applications. This domain contains application-layer protocols and integration with Business Intelligence (BI) systems.

Services layer

This layer is represented as a horizontal structure across industry-specific apps. Horizontal modules at this tier comprise the physical network on which IoT apps operate, the underlying management protocols, and the hardware. Examples include cellular backhaul communications, **Multiprotocol Label Switching** (**MPLS**) networks, **Virtual Private Networks** (**VPNs**), **Software Defined Networks** (**SDNs**), etc. The topmost layer is the common services layer.

Machine-To-Machine (M2M)

Machine-To-Machine, or M2M, is a term that describes any technology that enables networked devices to exchange data and carry out tasks without human intervention.

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching directs data between nodes based on specified labels and tags, not network addresses.

Software-Defined Networks (SDN)

Software-Defined Network (SDN) is a network architecture where the network is controlled through software-based controllers or Application Programming Interfaces (APIs) instead of specialized hardware devices.

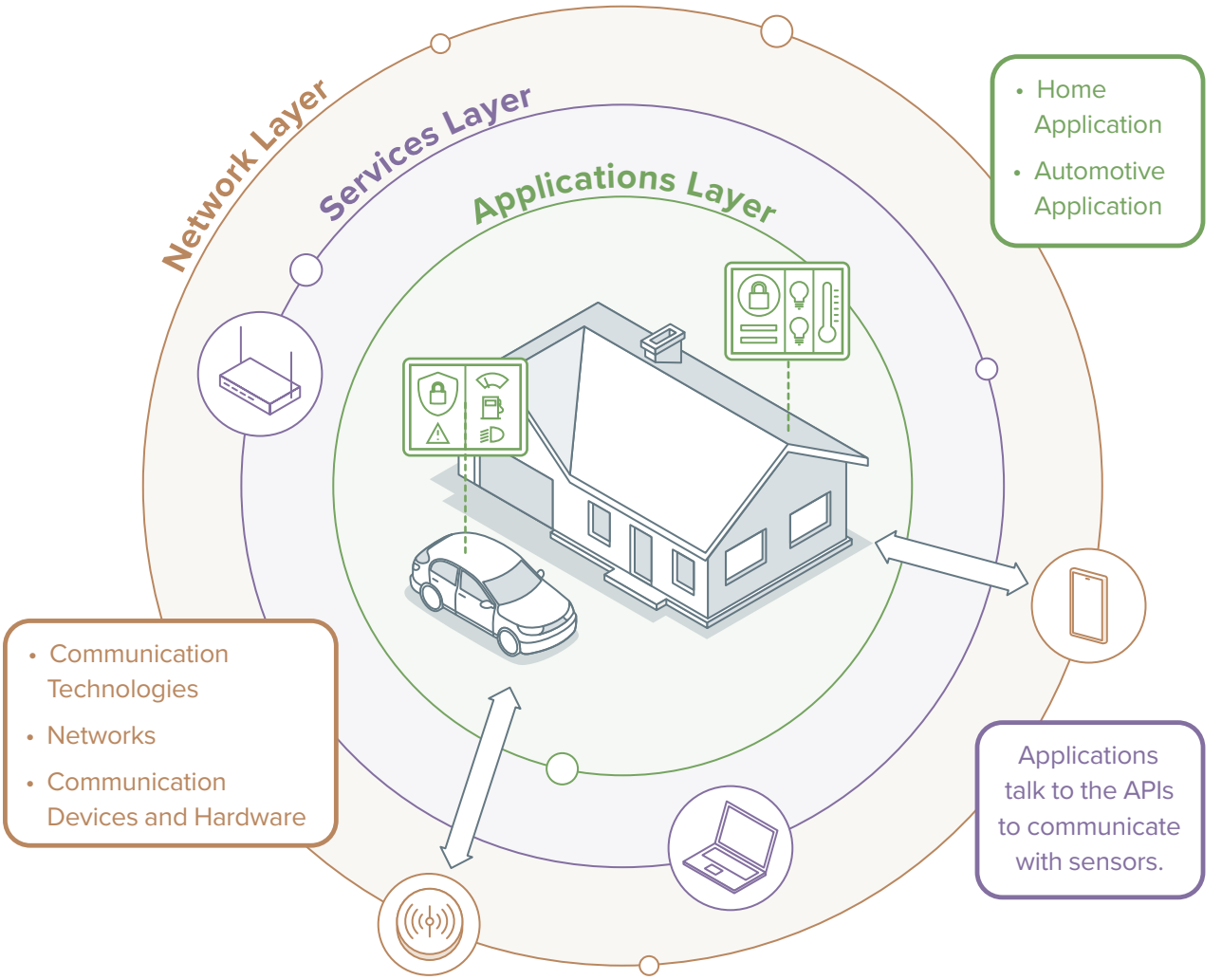
Network layer

This is the IoT devices and endpoints' communication domain. It consists of both the devices and the communications network that connects different types of networks like wireless mesh networks and **point-to-multipoint systems**.

Point-to-multipoint system

A point-to-multipoint system provides various pathways from a single network node to multiple destination nodes.

OneM2M Architecture Layers



Smart and non-smart gadgets frequently communicate with one another. In other cases, machine-to-machine communication is unnecessary, and devices merely connect with use case-specific apps in the IoT application domain across a Field Area Network (FAN). The FAN is the most complex component of the communications network since it is primarily responsible for providing "last-mile" communications to end devices. The device domain also consists of the gateway device, which provides connections to the core network and serves as the boundary between the device and network domains.

IoT World Forum Architecture

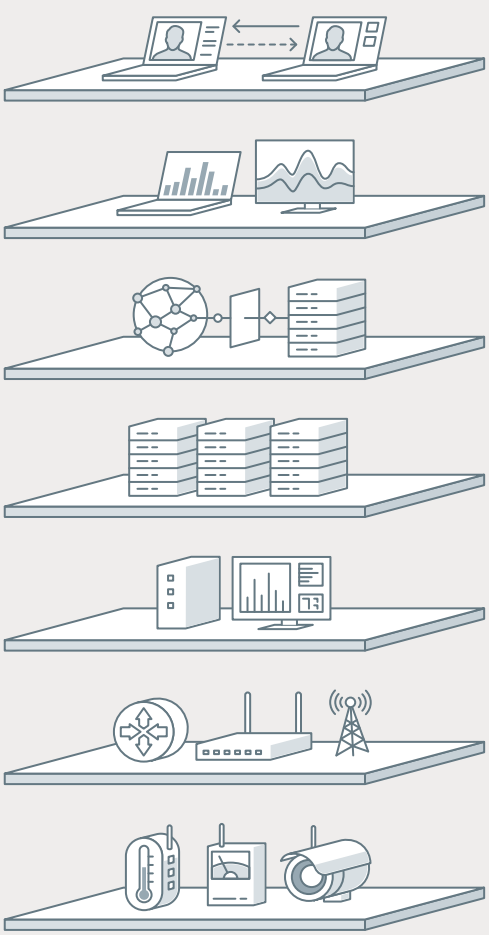
The IoT Reference Model introduced at the IoT World Forum specifies a series of levels with control flowing from a center point to edge layers, which consists of sensors, devices, machines, and other intelligent end nodes. In general, data moves from the edge layers of the stack to the center.

By utilizing this reference model, we may accomplish the following:

- Divide the IoT challenge into subproblems.
- Determine the various technologies at each layer and their interrelationships.
- Define a system whose components can be supplied by several vendors.
- Define interfaces in a manner that promotes interoperability.
- Define a layered security paradigm that is enforced at level transition points.

The IoT Reference Model is similar to the OSI Networking Model.

IoT World Forum Architecture Layers



Layers

7 Collaboration and processes
(Involving people and business processes)

6 Applications
(Reporting, analysis, and control)

5 Data abstraction
(Aggregation and access)

4 Data accumulation
(Storage)

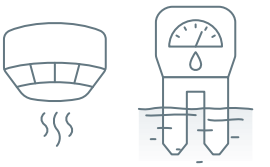
3 Edge computing
(Data element analysis and transformation)

2 Connectivity
(Communication and processing)

1 Physical devices and controllers
(The "Things" in IoT)

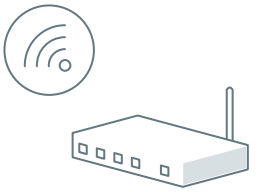
Layer 1: Physical devices and controllers layer

The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer contains the "things" of the Internet of Things, such as the many endpoint devices and sensors that send and receive data. These "things" can range in size from practically tiny sensors to enormous manufacturing machinery. Their main task is to generate data and allow control across a network.



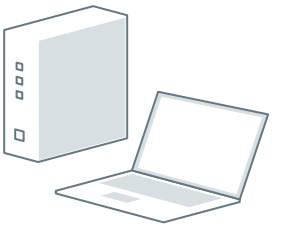
Layer 2: Connectivity layer

The role of the connectivity layer is the transfer of data in a reliable and timely manner. This covers transmissions between Layer 1 devices and the network, as well as transmissions between the network and Layer 3 information processing (the edge computing layer). As you may have noticed, the connection layer comprises all networking parts of IoT and makes no distinction between the last-mile network (the network between the sensor/endpoint and the IoT gateway, addressed later in this chapter), the gateway network, and the backbone network.



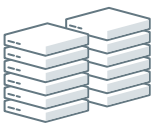
Layer 3: Edge computing

Edge computing falls under the responsibilities of Layer 3. This layer focuses on data reduction and transforming network data flows into information that is ready to be stored and processed by higher levels. One of the fundamental ideas of this reference model is that information processing is initinitiated as close to the network's edge as is feasible and as quickly as is possible. Layer 3 also performs the examination of data to determine whether it may be filtered or aggregated before being transferred to a higher layer. This also permits data to be reformatted or decoded, which facilitates further processing by other systems.



Layer 4: Data accumulation layer

This layer captures and stores data, making it accessible for programs whenever needed. Converts event-based data to formats that can be queried by other services.

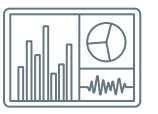


Layer 5: Data abstraction layer

Layer 5 reconciles diverse data formats and ensures consistent semantics from varied sources. Using virtualization, it verifies that the data set is full and consolidates data into a single location or several data stores.

Layer 6: Applications layer

The application layer utilizes software programs to interpret data. Applications are able to monitor, regulate, and generate reports depending on the data analysis.



Layer 7: Collaboration and processes layer

The last layer consumes and distributes application data. IoT's utility stems from the fact that sharing and collaborating on IoT data frequently involves numerous steps. This layer can alter company operations and offer IoT's advantages.

Short Range Communication Network and Protocols

RFID and NFC

Radio-Frequency Identification (**RFID**) and **Near-Field Communication** (**NFC**) are communication technologies that enable the short-range connection between IoT devices and a network. RFID and NFC are used to store and retrieve data remotely. They consist of a radio transponder, radio receiver, and radio transmitter and use electromagnetic fields to automatically recognize and track tags attached to smart objects. Each tag sends or receives digital data when activated by an electromagnetic interrogation pulse from a nearby RFID or NFC reader device.

RFID enables the tracking of tools, equipment, inventories, assets, and people through tags that are attached to them. If a tag is close to a reader, it can be read even if it is not visible. These tags can be read in bulk, unlike barcodes which can only be read one at a time, and they can be read within a case, carton, box, or another container.

NFC is generally used to exchange data between devices within a range of around 4 centimeters. It is used for contactless credit card transactions, to replace digital office or hotel keys, and to simplify the connection and setup of devices such as headphones.

The main difference between RFID and NFC is that NFC is designed for secure data exchange, making it appropriate for financial transactions, while RFID is mainly used for applications where we need to identify unique items wirelessly.

RFID vs NFC

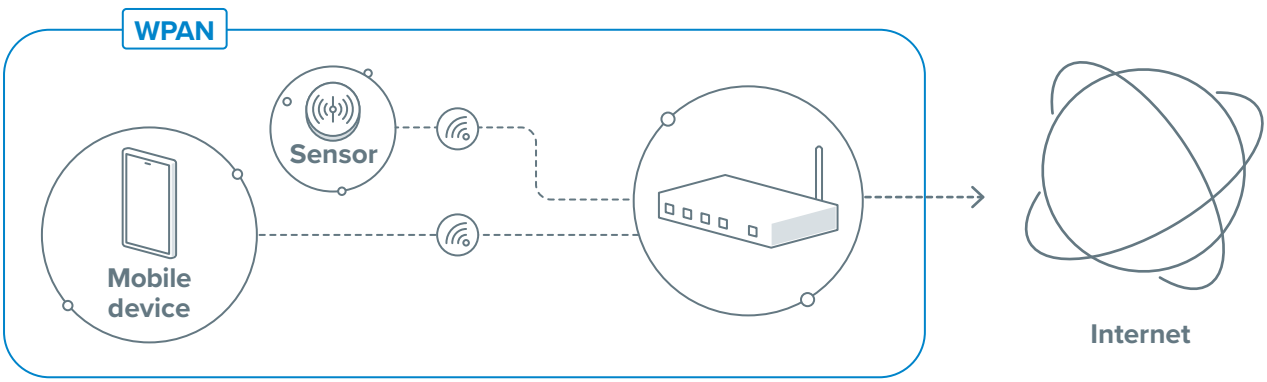
Feature	RFID	NFC
Usage frequency	125 kHz ~ 2.45 GHz	13.56 MHz
Connection range	Maximum 100 m	Within 10 cm (short distance)
Communication	One-way communication	Two-way communication
Advantage	Able to recognize over long distances	High security

Wireless Personal Area Networks (WPANS) and Protocols

Sensors and other Internet-connected objects require a means for transmitting and receiving data. This section discusses **Personal Area Networks** (**PAN**) and close-range communication. In an IoT ecosystem, sensors and actuators can communicate through copper lines or **Wireless Personal Area Networks** (**WPANs**).

Personal Area Network (PAN)

A Personal Area Network (PAN) is a computer network used to connect electronic devices within a user's workspace.



Non-IP Based WPANS Protocols

Zigbee

Zigbee is a WPAN protocol built on the IEEE 802.15.4 foundation, designed for cost-, power-, and space-constrained commercial and residential IoT networking. It can form networks, discover devices, secure the network, and manage it effectively. However, it does not offer data transport services or an application execution environment. Essentially, it functions as a self-healing mesh network.

The following table illustrates the main components of a Zigbee network.

Main components of a Zigbee network

Component	Description
Zigbee controller (ZC)	A highly capable device used to build and initiate network functions on a Zigbee network, able to assign logical network addresses and allow nodes to join or leave the mesh.
Zigbee router (ZR)	This optional component handles a portion of the mesh network by assigning logical network addresses and allowing nodes to join or exit the mesh.
Zigbee end device (ZED)	This is a simple straightforward endpoint device, such as a light switch or thermostat, that has the necessary capabilities to communicate with the coordinator.

Zigbee addresses three distinct data traffic types.

1. **Periodic data:** The rate of periodic data delivery or transmission is determined by the applications (for example, sensors periodically transmitting). When an application or external stimuli happens at a random pace, intermittent data is produced.


Sensor

2. **Intermittent data:** A light switch is a nice example of intermittent data ideal for Zigbee.

Light switch

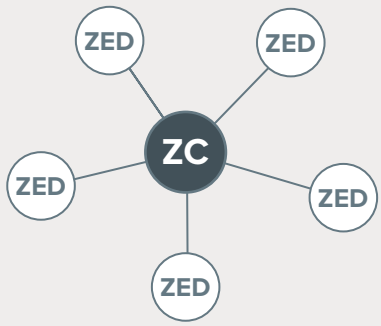
3. **Repeated low-latency data:** Zigbee assigns transmission time slots and can have very low latency, making it suitable for computer mice and keyboards.


Mouse

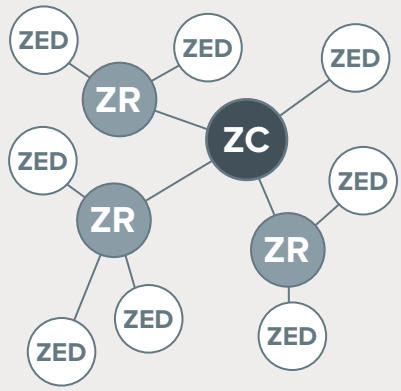
There are three fundamental Zigbee topologies:

Zigbee topologies

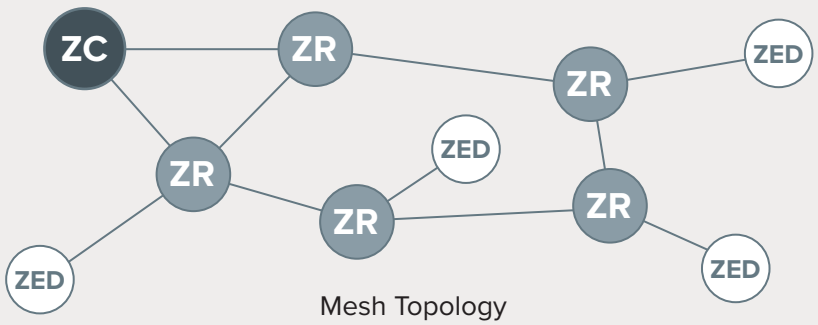
Component	Description
Star topology	A ZC containing one or more ZEDs. Only extends two **hops**, limiting the distance between nodes. A dependable link with a single point of failure at the ZC is also required.
Cluster tree topology	A multi-hop network that uses **beaconing** to extend coverage and range. ZEDs are endpoints, although ZC and ZR nodes can have child nodes. Child nodes communicate only with their parent nodes. Parent nodes can communicate upstream or downstream with their children. A central failure point remains a problem.
Mesh topology	Any source device can be routed to any destination device. Utilizes tree-based and table-based routing methods. To execute routing functions, ZC and ZR radios must be powered at all times, draining battery life. Routers within a specific range of each other are permitted to interact directly. The primary benefit is that the network may expand outside the line of sight and has redundant pathways.



Star Topology



Cluster Tree Topology



Mesh Topology

Hop

When a packet is passed from one network segment to the next, this is a hop.

Beaconing

Beaconing in networking is a periodic digital broadcast, like a lighthouse beacon.

Bluetooth

Bluetooth is a low-power wireless communication technology widely utilized in devices ranging from mobile phones to keyboards and gaming consoles. Bluetooth has been used extensively in IoT deployments for some time, as the primary device for beacons, wireless sensors, asset tracking systems, remote controls, health monitors, and alarms when operating in low energy mode (LE).

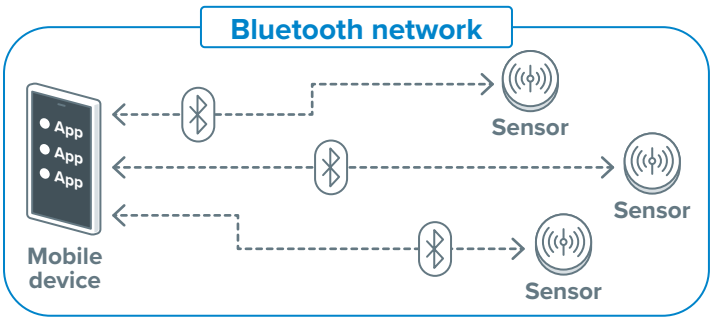
In a Bluetooth WPAN, a number of Bluetooth events can occur. The two fundamentals are:

Advertising
Initiated by a device to warn scanning devices of the existence of a device requesting to pair or relay a message contained in an advertising packet.

Connecting
This event describes the process of pairing a device with a host.

In Low Energy mode (LE), a device can carry out a complete communication utilizing only the advertising channel. Alternately, communication may involve pair-wise bidirectional communication and necessitate a formal connection between the devices. Devices required to make this sort of connection will begin the formation procedure by listening for advertising packets. In this situation, the listener is considered an initiator. If the advertiser transmits a connectable advertising event, the initiator may submit a connection request using the same physical channel it received the connectable advertising packet on.

The advertiser can then decide whether to establish a link. If a link is established, the advertising event concludes and the initiator is referred to as the master and the advertiser as the slave. Bluetooth terminology refers to this connection as a piconet, and connection events take place. The connection events between the master and slave all occur on the same beginning channel. After data has been transferred and the connection event has ended, frequency hopping can be used to select a new channel for the pair.



IP Based WPANS Protocols

6LoWPAN

IP networking over low-power RF communication systems is intended for devices with limited power and space that do not require high bandwidth networking services. The protocol is compatible with various WPAN communications, including IEEE.802.15.4, Bluetooth, and sub-1 GHz RF technologies, as well as Power Line Controller (PLC). The primary benefit of **6LoWPAN** is that even the most basic sensors may be IP-addressable and function as network citizens via 3G/4G/LTE/Wi-Fi/Ethernet routers. IPV6 can adequately cover an estimated 50 billion Internet-connected devices and continue to do so long into the foreseeable future. IPV6 is hence well-suited for IoT expansion.

6LoWPAN networks are mesh networks that exist on the outskirts of bigger networks. The topologies are adaptable, allowing for ad hoc and disjointed networks with no ties to the Internet or other systems, or they may be linked to the backbone or the Internet through edge routers. Various edge routers can connect multiple 6LoWPAN networks; this is known as multi-homing. In addition, ad hoc networks can emerge without the need for an edge router's Internet access.

Edge routers create 6LoWPAN mesh networks on the perimeters of larger, conventional networks. They can also facilitate IPV6-to-IPV4 swaps if necessary. Datagrams are handled similarly to an IP network, which offers some advantages over proprietary protocols. All nodes inside a 6LoWPAN network share the IPv6 prefix established by the edge router. Throughout the Network Discovery (ND) phase, nodes will register with the edge routers.

ND governs the interaction between hosts and routers in the local 6LoWPAN mesh. Multi-homing enables numerous 6LoWPAN edge routers to operate a network; for instance, when failover or fault tolerance requires various media (4G and Wi-Fi).

Thread

Thread is an IoT networking protocol based on IPV6 (6LoWPAN). Its primary objective is home automation and home networking. Thread is IP-addressable and is based on the IEEE 802.15.4 protocol and 6LoWPAN. It shares similarities with Zigbee and other 802.15.4 variations but differs significantly in that it is IP-addressable. This IP protocol is based on the data and physical layers of 802.15.4 and the security and routing characteristics of 6LoWPAN.

Thread is also mesh-based, making it a viable option for residential lighting systems with up to 250 devices per mesh. The advantage of Thread is that by providing IP addressability in very small sensors and home automation systems, one may reduce power consumption because the protocol does not require application state persistence at the network layer. This also means that the edge router hosting a Thread mesh network does not need to handle application layer protocols, hence reducing its power and processing requirements. Being IPV6 compatible and having all communications encrypted using the Advanced Encryption Standard (AES), it is naturally secure.

Long Range Communication Networks and Protocols

Wireless Personal Area Networks (WPAN) and Wireless Local Area Networks (WLAN) link sensors to a local network but not necessarily to the Internet or other systems. The IoT ecosphere will encompass sensors, actuators, cameras, smart-embedded gadgets, vehicles, and robots at the most remote locations. In the long term, we must deal with the Wide Area Network (WAN).

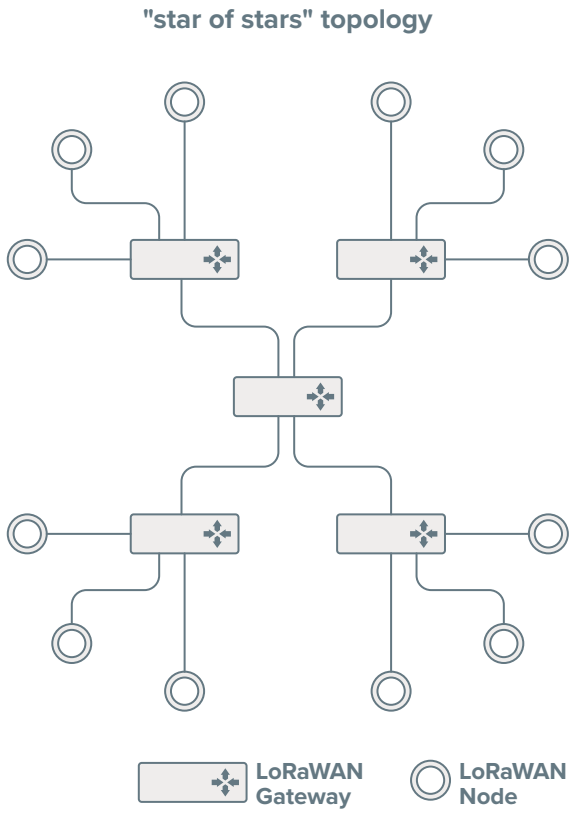
LoRaWAN

Low-Power Wide-Area (LPWA) wireless technologies are ideally suited for long-range and battery-powered endpoints. Frequently, **LoRaWAN** topology is referred to as "star of stars" topology. Endpoints exchange packets via gateways functioning as bridges, with a central LoRaWAN network server. Endpoints communicate directly with one or more gateways, whereas gateways connect to the backend network via regular IP connections.

The same packets can be received and transported by many gateways. When duplicate packets are received, the network server is responsible for de-duplication.

Unlicensed LPWA technologies give new options for private corporate networks, broadcasters, and mobile and non-mobile service providers to deploy IoT infrastructures, solutions, and use cases. The ecosystem of endpoints is expanding fast and will undoubtedly be the deciding factor between the various LPWA technologies and solutions, such as LoRaWAN.

Smart-city operators, broadcasters, and mobile and non-mobile service providers are addressing the need for regional or national IoT infrastructures, which are vital for enabling use cases for consumer markets.



Cellular networks (5G)

The most common kind of communication is cellular radio, especially cellular data. Prior to the development of cellular technology, mobile communication devices had limited coverage, shared frequency space, and were effectively two-way radios. Cellular Networks are excellent at carrying data in both directions at fast speeds but at the expense of range and battery consumption.

5G is the next-generation IP-based communication technology that is being developed to succeed 4G cellular networks. Additionally, 5G enhances bandwidth, latency, density, and user expense.

5G aims to be a single umbrella standard that encompasses all cellular services and categories, as opposed to building distinct services and categories for each use case.

Main features of modern 5G networks

Features	Description
	Enhanced Mobile Broadband (eMBB)
	Ultra-Reliable and Low-Latency Communications (URLLC)
	Massive Machine Type Communications (mMTC)

EXERCISES

1 Choose the correct answer.

1. What is the range of NFC technologies used for communication between devices?

   A. Long range

   B. Short range

   C. Medium range

   D. Global range

2. Which layer does the oneM2M architecture contain?

   A. Application layer

   B. Data layer

   C. Network layer

   D. Transport layer

3. What is required for smart city network systems?

   A. Long Range Communication Networks and Protocols are not needed

   B. Only short-range communication technologies

   C. Long Range Communication Networks and Protocols are needed

   D. Exclusive use of wired communications

2 Classify the key layers of the oneM2M architecture for IoT systems.

3 Analyze the main layers of the IoT World Forum system architecture.

4 Identify the main characteristics of RFID and NFC technologies.

5 Identify the three key components of a Zigbee network.

6 Define the "star of stars" topology that LoRaWAN networks use.

LESSON 3

Security and Privacy of IoT Systems

Security

Internet, IoT, Cloud-Based Services, **Cyber-Physical Systems** (**CPSs**), and mobile devices define modern life in the 21st century. Technology allows worldwide communication, which benefits society. However, as technology evolves, cybercriminals can exploit more vulnerabilities. IoT's impact on enterprises and business models is growing. The success of IoT for businesses depends on consumer trust. Nevertheless, many technological products and services are rushed to market with low concern for users' security and privacy.

Security is a critical part of the design process from the starting level to each next level. Security policies, protocols, and standards must be created in parallel to support any technological development.

The following table presents IoT security principles.

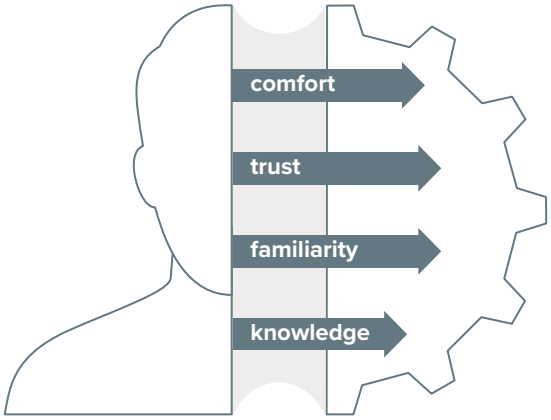
Cyber-Physical System (CPS)

A Cyber-Physical System (CPS) is a computer system that controls or monitors a mechanism using computer-based algorithms.

IoT security principles

Principle	Description
 Trust	Allow only authorized users or services to access the device or data.
 Identity	Verify the identity of individuals, services, and "things".
 Privacy	Maintain the privacy of a user's device, personal information, and sensitive data.
 Protection	Safeguard devices and users against physical, financial, and reputational harm.

User-Centered Challenges Of IoT Systems



Traditional security measures are insufficient to provide comprehensive security to the modern connected world. Unlike many traditional electronic devices, IoT devices interact with services on the Internet. Many potential benefits will not be realized until people become comfortable with these technologies. Accountability is critical for trust between end-users and the creators of IoT systems. The complexity of distributed data flows, inadequate consent mechanisms, and a lack of information to the user all contribute to the need to build accountability into the IoT.

IoT Security and Cybercrime

Internet infrastructure is a physical construct inside sovereign nations' territorial boundaries. Nonetheless, the data flowing over this infrastructure traverses several national jurisdictions, which remains a cyberspace-specific concern. While illegal conduct in cyberspace easily crosses geographical borders, law enforcement does not.

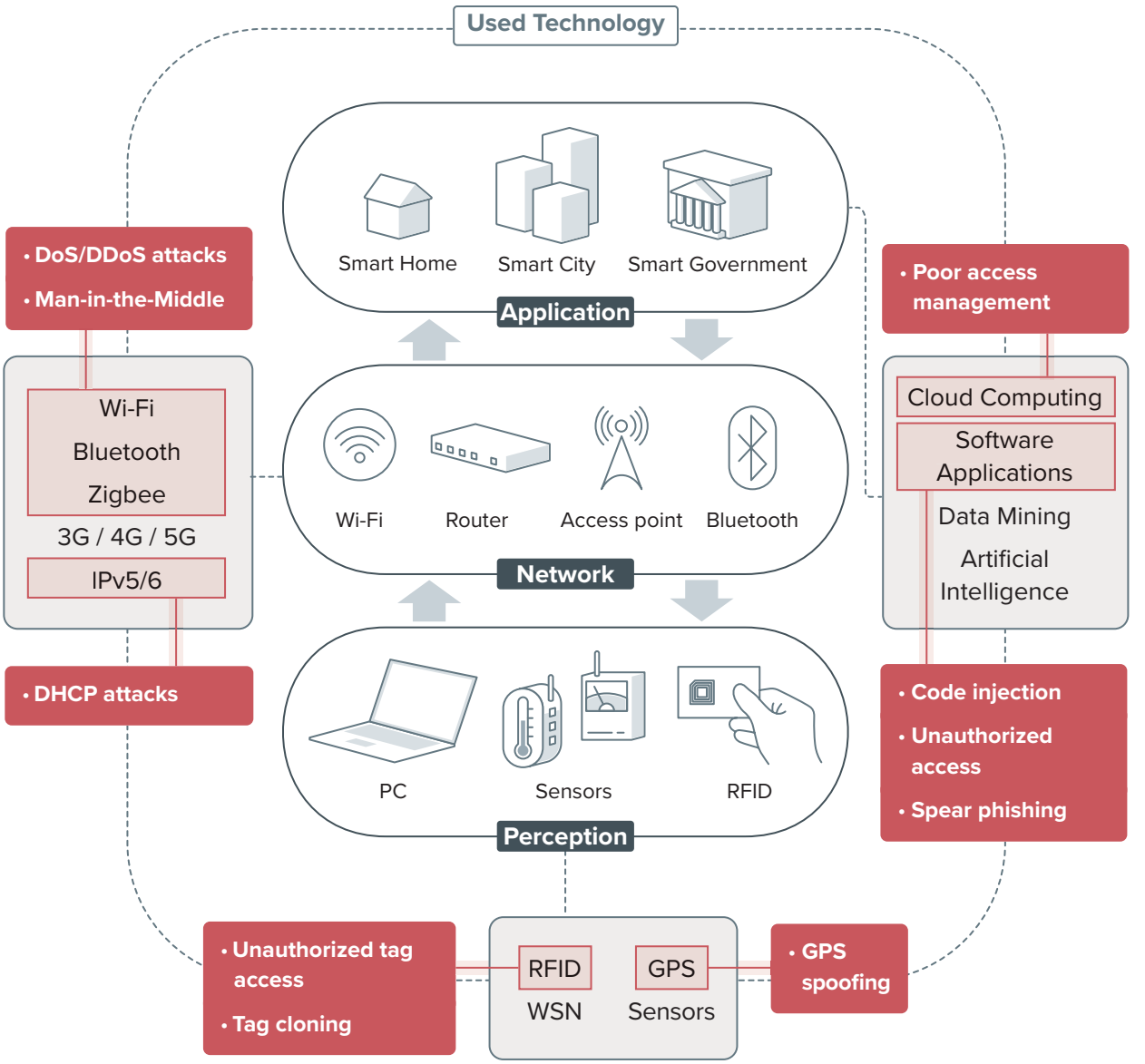
The gap between legislation and technology is a major obstacle in combating cybercrime. The criminal justice system is inherently retrospective and time-consuming, creating significant difficulties for cyberspace regulation. The rate at which technology is integrated into our society outpaces the creation of policy and legislation. As a result, cyberspace is controlled by a patchwork of inadequate, underdeveloped, and competing laws.

Additionally, a consensus is difficult to achieve because each nation has its autonomous norms, beliefs, and practices, promoting different visions for cyberspace. Various nations, for instance, promote cyber sovereignty, arguing that national borders apply to cyberspace and that each nation should be able to regulate how individuals and corporations use the Internet within its borders.

Architectural Challenges of IoT Security

IoT requires a set of standards and a well-defined architecture with interfaces, data models, and protocols due to the variety of devices, protocols, and services involved. Numerous attacks are possible when IoT devices connect with a cloud service and exchange data for the first time. Various IoT device characteristics might pose security risks and issues. Mobility, interdependence, and other similar characteristics introduce various challenges and dangers, such as firmware vulnerabilities, storage, processing power, network attacks, rules, and standards, that necessitate additional study. The Internet of Things necessitates more IPv4-to-IPv6 transitioning devices, necessitating an increase in bandwidth. The adoption of IPv6 and 5G, as well as the new generation of communication for improved speed, generate additional risks and difficulties.

The following illustrations demonstrate how a simple architecture evolves from a simple system to an increasingly complex one. Each layer of complexity has new vulnerabilities to the system's components.



5G Networks and IoT Security

5G is a promising technology that has been identified as the next step in the global evolution of mobile communication over the long term. 5G is the primary component of a networked or IoT/M2M-oriented society. It will enable fast access to information and services. The objective of 5G is mobile connectivity for humans as well as mobile and ubiquitous connectivity for any computing device and application that can benefit from being connected to the Internet (IoT) and the Web (WoT—Web of Things).

The development of 5G networks raises concerns about the impact on IoT device communication security. There will be a need for IoT middleware and a security standard to implement new methods for interconnecting various cognitive networks and devices. With a better and faster network infrastructure, there will be greater interaction between things, particularly with the distribution of processing for cloud services, generating a high impact in terms of data security and enabling the development of new applications that improve people's lives.

The following table illustrates the main IoT 5G security concerns.

IoT 5G security concerns

Concern	Description
 Big data security	IoT systems continuously create large amounts of heterogeneous data. In addition, data traffic demands for mobile communication in IoT systems will expand considerably. Therefore, it is necessary to devise an effective method for managing these large amounts of data created by IoT systems. 5G network technologies deliver data at a substantially lower cost per bit than previous networks. Secure protocols are needed to properly manage and organize these massive amounts of data to establish a comprehensive security solution for a 5G-based IoT system.
 Device and application protection	Protecting numerous devices and applications is an additional difficulty. A crucial feature of 5G-based IoT systems is the potential to support a far larger number of devices and applications than is now possible. The connections of millions of additional devices and applications will introduce new security concerns. Even with a simple cyberattack, victims could be locked out of their homes, cars, and other linked devices.
 Communication channels protection	Maintain the privacy of a user's device, personal information, and sensitive data.

Privacy

While online security remains a major concern and challenge in the IoT environment, preserving privacy will also remain a significant challenge that requires additional attention. The privacy of IoT end-users could be jeopardized if personal data is leaked to unauthorized parties. Given the diversity of IoT-connected devices and the inherent vulnerabilities of hardware and software in some of them, protecting end-user privacy may present numerous security challenges.

The vast amount of personal data collected by big data systems allows organizations to combine different datasets, increasing the ability to identify individuals. The capacity to mine and analyze datasets grows in volume and variability daily. To address this challenge, it is prudent to ensure that personal data is completely anonymized. Organizations that use anonymized data must demonstrate that they conducted a thorough risk assessment and implemented effective security techniques. This could include a variety of technical safeguards, such as **data masking** and **pseudonymization**, as well as legal and organizational safeguards.

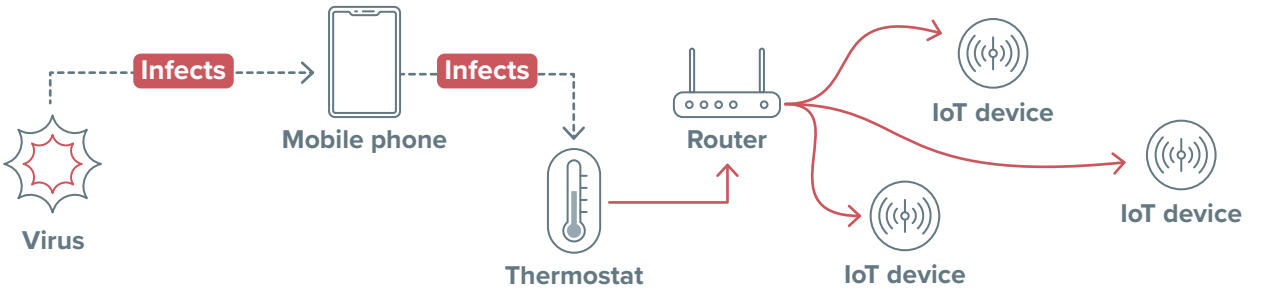
Data masking

Data masking is the process of changing sensitive data. The data is of no value to unauthorized intruders but is still usable by software and authorized personnel for further analysis.

Pseudonymization

Pseudonymization is a data management and de-identification process that replaces personally identifiable information fields in a data record with one or more pseudonyms.

Infection of a network



Example

Hackers can compromise an IoT network and collect private data by exploiting **Universal Plug and Play** (**UPnP**) devices. UPnP offers zero configuration, meaning no authentication is required to connect. Hackers exploit this feature to infect a device and then an IoT network. For example, a mobile phone infected with a virus could connect to a thermostat in your smart home residence through Wi-Fi. This thermostat is connected through UPnP to the router of your smart home. The whole IoT network is infected with this virus, and now a data breach of private information has occurred.

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is a service that enables devices on the same local network to automatically find and connect to each other using standard networking protocols. Printers, routers, mobile devices, and smart TVs are all types of UPnP devices.

Personal Sensitive Data
This is the full data including personal and special data

Name	John Smith
Date of birth	24.02.84
Email	Johns@mail.com
User ID	JSmith_84
Health	Type 1 diabetes

Pseudonymous Data
IDs are replaced and sensitive data is encrypted.

Name	User 458230
Date of birth	24.02.84
Email	#Sd24@!04gTu
User ID	%UTopRg#Ku!1
Health	Type 1 diabetes

Anonymous Data
IDs removed and sensitive data randomized/generalized

Sex	Male
Age	30–49
Health	Type 1 diabetes

Data protection and security are difficult in an IoT environment because at the system's core is a communication interface between smart objects without human intervention. Given the rate of the evolution of such systems, it is not surprising that there is little evidence to suggest that data protection is keeping up. Even when legislators demonstrate an awareness of specific concerns in large-scale data processing, their understanding of risk implications may be insufficient in practice.

The following table presents the current IoT privacy concerns and their possible solutions.

IoT privacy concerns and their possible solutions

Privacy concerns	Possible solutions
Data collection from various sources without careful verification of relevance or accuracy.	Utilize AI to validate the accuracy of acquired data.
Big data approaches enable organizations to merge multiple datasets, which enhances the possibility that data may identify living individuals.	Utilize a variety of technical precautions, such as data masking, anonymization, pseudonymization, and aggregation, in addition to legal and organizational safeguards.
The lack of openness in data processing and the complexity of Big Data analytics might contribute to mistrust.	Improve the level of openness by providing privacy disclosures before processing any data obtained.
The difficulty of determining if new uses are consistent with the original intent of data collection.	An organization may collect personal data for one purpose and subsequently analyze it for a completely different purpose. In such a case, the users must be informed of the change, and if necessary, further consent must be acquired.
Any breaches will threaten users' privacy and harm the creators' credibility, decreasing trust and causing users to lose faith in the organization and system.	Technical methods like encryption protocols and blockchain technology are utilized. Access control, video surveillance, and security records are physical security systems that can be implemented.
Design of systems with privacy protection in mind.	A privacy risk assessment will give an early warning system for detecting privacy issues.
Lack of IoT-related national, regional, and global policies and regulatory frameworks, which can also conflict with technological development.	It is essential to bring together nations, international organizations, industrial partners, and security and IoT experts from industry and academia to develop solutions to protect IoT-generated personal data.

EXERCISES

1 Choose the correct answer.

1. How are cybersecurity laws implemented across countries?
   - **A.** The same way in each country
   - **B.** Differently in each country
   - **C.** Not at all in most countries
   - **D.** Universally across all countries without changes
2. How is personal data handled by smart objects typically?
   - **A.** It is automatically encrypted
   - **B.** It is never encrypted
   - **C.** It may or may not be encrypted
   - **D.** It is always public
3. What do pseudonymization techniques do?
   - **A.** Introduce fake data to protect the real data
   - **B.** Encrypt data
   - **C.** Remove all data
   - **D.** Store data without changes

2 Classify the main principles of IoT security.

3 Describe the main challenge of IoT security and cybercrime on the Internet. Suggest how this issue be addressed.

4 Distinguish various types of possible attacks on every layer of a simple IoT architecture.

5 Describe the most significant technological security challenge created by 5G networks in IoT systems.

PROJECT

Privacy and Protection in Smart Healthcare

Smart healthcare is one of the most important sectors that IoT technologies improve. A variety of devices and systems are interconnected and exchange large amounts of data. Medical and biological data are considered the most private personal data and must be protected by companies and governments.

1. In traditional healthcare, medical and biological data would be used by the patient, their doctors, hospitals, and medical centers. In smart healthcare, this data can be accessed from many more points. Write down the types of devices, services, and systems that transport, process, or store personal biological data through smart healthcare systems.

2. Technology companies that build IoT systems are not the only ones responsible for protecting biological data. Governments are accountable for providing legislation and regulation to protect citizens from personal data misuse or breach. Search the Internet for examples of legislation of your country for smart healthcare systems. Search the Internet for similar legislation provided by another country of your choosing.

3. After you have written down your notes, use them to create a PowerPoint presentation that demonstrates the potential issues of security and privacy in smart healthcare and the difference in legislation between your country and another country of your choosing.

WRAP UP

THIS UNIT COVERED HOW TO:

> describe how body sensor networks are utilized in smart healthcare applications.

> define the types of UAV sensors that are used in smart agriculture IoT applications.

> identify the main domains of the oneM2M architecture.

> distinguish the different layers of the IoT World Forum architecture.

> identify the differences between NFC and RFID technologies.

> identify the networking protocols that are used in Wireless Personal Area Networks (WPANS).

> classify the main principles of IoT security.

> identify security techniques that are established in IoT privacy.

KEY TERMS

- 6LoWPAN
- Bluetooth
- Body Sensor Network
- Data Masking
- Edge Computing
- Electrocardiogram
- Electroencephalogram
- Electromyography
- Internet of Healthcare Things
- IoT World Forum Architecture
- LoRaWAN
- Low-Power Wide-Area (LPWA)
- NFC
- oneM2M Architecture
- Personal Area Network (PAN)
- Pseudonymization
- RFID
- Thread
- UAV
- Virtual Private Network (VPN)
- Wireless Personal Area Network (WPAN)
- Wireless Sensor Network (WSN)
- Zigbee

Foundations of IoT

Internet of Things 2

Create, connect, communicate

Imagine designing smart devices that communicate seamlessly with each other or building a secure, thriving e-commerce store that attracts and retains customers. What if you could create connected systems that make everyday life easier, from home automation to advanced security solutions?

Foundations of IoT: The Internet of Things 2 introduces you to the fundamentals of both the Internet of Things (IoT) and e-commerce. Learn to create connected devices using tools like Arduino, from smart homes to security systems. Master the strategies to build and secure your own online store, drive traffic with SEO, email campaigns, and social media, and ensure secure transactions.

By the end, you'll have the skills to design, secure, and promote your own IoT applications or e-commerce business with confidence, connecting the world and shaping the future.

Mc Graw Hill

binarylogic

ISBN-13: 978-1-2659-0286-5
ISBN-10: 1-2659-0286-0

9 781265 902865