Unit 8: Internet of Things: An Introduction

8.1. Introduction to IoT

Internet of Things (IoT) is a massive network of physical devices embedded with sensors, software, electronics, and network which allows the devices to exchange or collect data and perform certain actions.

Simply put, IoT is made up of two words: **Internet** & **Things**.

- Things – physical devices, appliances, gadgets, etc.
- Internet – through which these devices are connected

IoT aims at extending internet connectivity beyond computers and smartphones to other devices people use at home or for business. The technology allows devices to get controlled across network infrastructure remotely. As a result, it cuts down the human effort and paves the way for accessing the connected devices easily. With autonomous control, the devices are operable without involving human interaction. IoT makes things virtually smart through AI algorithms, data collection, and networks enhancing our lives.

Examples: Pet tracking devices, diabetes monitors, AC sensors to adjust the temperature based on the outside temperature, smart wearables, and more.

IoT comprises things that have unique identities and are connected to internet. By 2020 there will be a total of 50 billion devices /things connected to internet. IoT is not limited to just connecting things to the internet but also allow things to communicate and exchange data. Definition: A dynamic global n/w infrastructure with self -configuring capabilities based on standard and interoperable communication protocols where physical and virtual ―things‖ have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information n/w, often communicate data associated with users and their environments.

8.2.Characteristics of IoT

1) **Dynamic & Self Adapting:** IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user‗s context or sensed environment. Eg: the surveillance system is adapting itself based on context and changing conditions.
2) **Self Configuring:** allowing a large number of devices to work together to provide certain functionality.
3) **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.
4) **Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address).
5) **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

8.3. IoT Categories:

1. *Consumer IoT (CIoT)* refers to the use of IoT for consumer applications and devices. Common CIoT products include smartphones, wearables, smart assistants, home appliances, etc. Typically, CIoT solutions leverage Wi-Fi, Bluetooth, and ZigBee to facilitate connectivity. These technologies offer short-range communication suitable for deployments in smaller venues, such as homes and offices.

While CIoT tends to focus on augmenting personal and home environments, Commercial IoT goes a bit further, delivering the benefits of IoT to larger venues. Think: commercial office buildings, supermarkets, stores, hotels, healthcare facilities, and entertainment venues.

There are numerous use cases for commercial IoT, including monitoring environmental conditions, managing access to corporate facilities, and economizing utilities and consumption in hotels and other large venues. Many Commercial IoT solutions are geared towards improving customer experiences and business conditions.

2. Industrial IoT (IIoT), is perhaps the most dynamic wing of the IoT industry. Its focus is on augmenting existing industrial systems, making them both more productive and more efficient. IIoT deployments are typically found in large-scale factories and manufacturing plants and are often associated with industries like healthcare, agriculture, automotive, and logistics. The Industrial Internet is perhaps the most well-known example of IIoT.

3. *Infrastructure IoT* is concerned with the development of smart infrastructures that incorporate IoT technologies to boost efficiency, cost savings, maintenance, etc. This includes the ability to monitor and control operations of urban and rural infrastructures, such as bridges, railway tracks, and on- and offshore windfarms. Technically speaking, infrastructure IoT is a subset of IIoT. However, due to its significance, it’s often treated as its own separate thing.
4. The last type of IoT is the *Internet of Military Things (IoMT),* often referred to as Battlefield IoT, the Internet of Battlefield Things, or simply IoBT. IoMT is precisely what it sounds like — the use of IoT in military settings and battlefield situations. It is chiefly aimed at increasing situational awareness, bolstering risk assessment, and improving response times. Common IoMT applications include connecting ships, planes, tanks, soldiers, drones, and even Forward Operating Bases via an interconnected system. In addition, IoMT produces data that can be leveraged to improve military practices, systems, equipment, and strategy.

8.4. IoT Enablers and Connectivity Layers

System installers, repairers, craftsmen, electricians, plumbers, architects who connect devices and systems to the Internet for personal use and for commercial and other business uses.

As the Internet of Things (IoT) enables devices to make intelligent decisions that generate positive business outcomes, it’s the sensors that enable those decisions. As cost and time-to-market pressures continue to rise, sensors provide greater visibility into connected systems and empower those systems to react intelligently to changes driven by both external forces and internal factors. Sensors are the components that provide the actionable insights that power the IoT and enable organizations to make more effective business decisions. It’s through this real-time measurement that the IoT can transform an organization’s ability to react to change.

.

Wi-Fi was designed for computers, and 4G LTE wireless targeted smartphones and portable devices. Both have been tremendously successful — and both were shaped by the devices they were intended for. The same goes for 5G, the first generation of wireless technology designed with extremely small, low-power, and near-ubiquitous IoT devices in mind. Unlike Wi-Fi and LTE devices, which we handle and plug into power sources on a daily basis, IoT sensors will operate autonomously for years at a time, often in inaccessible places, without recharging or replacement. An explosion of new protocols: The IoT is prompting the development of a number of different 5G communication standards, not just one or two network types

8.4.Baseline Technologies of IoT

According to Jones, the top 10 emerging IoT technologies are:

1. IoT Security: Security technologies will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating "things" or denial-of-sleep attacks that drain batteries. IoT security will be complicated by the fact that many "things" use simple processors and operating systems that may not support sophisticated security approaches.

2. IoT Analytics: IoT business models will exploit the information collected by "things" in many ways, which will demand new analytic tools and algorithms. As data volumes increase over the next five years, the needs of the IoT may diverge further from traditional analytics.

3. IoT Device (Thing) Management: Long-lived nontrivial "things" will require management and monitoring, including device monitoring, firmware and software updates, diagnostics, crash analysis and reporting, physical management, and security management. Tools must be capable of managing and monitoring thousands and perhaps even millions of devices.

4. Low-Power, Short-Range IoT Networks. Low-power, short-range networks will dominate wireless IoT connectivity through 2025, far outnumbering connections using wide-area IoT networks. However, commercial and technical trade-offs mean that many solutions will coexist, with no single dominant winner.

5. Low-Power, Wide-Area Networks. Traditional cellular networks don't deliver a good combination of technical features and operational cost for those IoT applications that need wide-area coverage combined with relatively low bandwidth, good battery life, low hardware and operating cost, and high connection density. Emerging standards such as narrowband IoT will likely dominate this space.

6. IoT Processors. The processors and architectures used by IoT devices define many of their capabilities, such as whether they are capable of strong security and encryption, power consumption, whether they are sophisticated enough to support an operating system, updatable firmware, and embedded device management agents. Understanding the implications of processor choices will demand deep technical skills.

7. IoT Operating Systems. Traditional operating systems such as Windows and iOS were not designed for IoT applications. They consume too much power, need fast processors, and in some cases, lack features such as guaranteed real-time response. They also have too large a memory footprint for small devices and may not support the chips that IoT developers use. Consequently, a wide range of IoT-specific operating systems has been developed to suit many different hardware footprints and feature needs.

8. Event Stream Processing: Some IoT applications will generate extremely high data rates that must be analyzed in real time. Systems creating tens of thousands of events per second are common, and millions of events per second can occur in some situations. To address such requirements, distributed stream computing platforms have emerged that can process very high-rate data streams and perform tasks such as real-time analytics and pattern identification.

9. IoT Platforms. IoT platforms bundle many of the infrastructure components of an IoT system into a single product. The services provided by such platforms fall into three main categories:

Low-level device control and operations such as communications, device monitoring and management, security, and firmware updates; IoT data acquisition, transformation and management; IoT application development, including event-driven logic, application programming, visualization, analytics and adapters to connect to enterprise systems.

10.IoT Standards and Ecosystems. Standards and their associated application programming interfaces (APIs) will be essential because IoT devices will need to interoperate and communicate, and many IoT business models will rely on sharing data between multiple devices and organizations. Many IoT ecosystems will emerge, and organizations creating products may have to develop variants to support multiple standards or ecosystems and be prepared to update products during their life span as the standards evolve and new standards and APIs emerge.

8.5.Sensors

Sensors are used for sensing things and devices etc. A sensor is a device that provides a usable output in response to a specified measurement. The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity. The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance etc.

8.6.1. Characteristics of a Sensor

The static accuracy of a sensor indicates how much the sensor signal correctly represents the measured quantity after it stabilizes (i.e. beyond the transient period.) Important **static characteristics** of sensors include sensitivity, resolution, linearity, zero drift and full-scale drift, range, repeatability and reproducibility.

1. *Sensitivity* is a measure of the change in output of the sensor relative to a unit change in the input (the measured quantity.) Example: The speakers you purchase for your home entertainment may have a rated sensitivity of 89 dB Signal Pressure Level per Watt per meter.

2. *Resolution* is the smallest amount of change in the input that can be detected and accurately indicated by the sensor. Example: What is the resolution of an ordinary ruler? of a Vernier Calipers?

3. *Linearity* is determined by the calibration curve. The static calibration curve plots the output amplitude versus the input amplitude under static conditions. Its degree of resemblance to a straight line describes the linearity.

4. *Drift* is the deviation from a specific reading of the sensor when the sensor is kept at that value for a prolonged period of time. The *zero drift* refers to the change in sensor output if the input is kept steady at a level that (initially) yields a zero reading. Similarly, the *full -scale drift* is the drift if the input is maintained at a value which originally yields a full scale deflection. Reasons for drift may be extraneous, such as changes in ambient pressure, humidity, temperature etc., or due to changes in the constituents of the sensor itself, such as aging, wear etc.

5. The *range* of a sensor is determined by the allowed lower and upper limits of its input or output. Usually the range is determined by the accuracy required. Example:

Sometimes the range may just be determined by physical limitations. Example: a pocket ruler.

6. *Repeatability* is defined as the deviation between measurements in a sequence when the object under test is the same and approaches its value from the same direction each time. The measurements have to be made under a short enough time duration so as not to allow significant long term drift. Repeatability is usually specified as a percentage of the sensor range. Example:

7. *Reproducibility* is the same as repeatability, except it also incorporates long time lapses between subsequent measurements. The sensor has to be operation between measurements, but must be calibrated. Reproducibility is specified as a percentage of the sensor range per unit of time.

The **dynamic characteristics** of a sensor represent the time response of the sensor system. Knowledge of these is essential to fruitfully use a sensor. Important common dynamic responses of sensors include rise time, delay time, peak time, settling time percentage error and steady-state error

8.6.2. Classification of Sensors

The common IoT sensors include:

Temperature sensors, Pressure sensors, Motion sensors, Level sensors, Image sensors, Proximity sensors, Water quality sensors, Chemical sensors, Gas sensors, Smoke sensors, Infrared (IR) sensors, Humidity sensors, etc.

A description of each of these sensors is provided below.

Temperature sensors

Temperature sensors detect the temperature of the air or a physical object and concert that temperature level into an electrical signal that can be calibrated accurately reflect the measured temperature. These sensors could monitor the temperature of the soil to help with agricultural output or the temperature of a bearing operating in a critical piece of equipment to sense when it might be overheating or nearing the point of failure.

Pressure sensors

Pressure sensors measure the pressure or force per unit area applied to the sensor and can detect things such as atmospheric pressure, the pressure of a stored gas or liquid in a sealed system such as tank or pressure vessel, or the weight of an object.

Motion sensors

Motion sensors or detectors can sense the movement of a physical object by using any one of several technologies, including passive infrared (PIR), microwave detection, or ultrasonic, which uses sound to detect objects. These sensors can be used in security and intrusion detection systems, but can also be used to automate the control of doors, sinks, air conditioning and heating, or other systems.

Level sensors

Level sensors translate the level of a liquid relative to a benchmark normal value into a signal. Fuel gauges display the level of fuel in a vehicle’s tank, as an example, which provides a continuous level reading. There are also point level sensors, which are a go-no/go or digital representation of the level of the liquid. Some automobiles have a light that illuminates when the fuel level tank is very close to empty, acting as an alarm that warns the driver that fuel is about to run out completely.

Image sensors

Image sensors function to capture images to be digitally stored for processing. License plate readers are an example, as well as facial recognition systems. Automated production lines can use image sensors to detect issues with quality such as how well a surface is painted after leaving the spray booth.

Proximity sensors

Proximity sensors can detect the presence or absence of objects that approach the sensor through a variety of different technology designs.

Water quality sensors

The importance of water to human beings on earth not only for drinking but as a key ingredient needed in many production processes dictates the need to be able to sense and measure parameters around water quality. Some examples of what is sensed and monitored include:

Chemical presence (such as chlorine levels or fluoride levels),Oxygen levels (which may impact the growth of algae and bacteria),Electrical conductivity (which can indicate the level of ions present in water), pH level (a reflection of the relative acidity or alkalinity of the water),Turbidity levels (a measurement of the amount of suspended solids in water)

Chemical sensors

Chemical sensors are designed to detect the presence of specific chemical substances which may have inadvertently leaked from their containers into spaces that are occupied by personnel and are useful in controlling industrial process conditions.

Gas sensors

Related to chemical sensors, gas sensors are tuned to detect the presence of combustible, toxic, or flammable gas in the vicinity of the sensor. Examples of specific gases that can be detected include:

Bromine (Br_2), Carbon Monoxide (CO), Chlorine (Cl_2), Chlorine Dioxide (ClO_2),Hydrogen Cyanide (HCN),Hydrogen Peroxide (H_2O_2), Hydrogen Sulfide (H_2S), Nitric Oxide (NO), Nitrogen Dioxide (NO_2), Ozone (O_3), etc.

Smoke sensors

Smoke sensors or detectors pick up the presence of smoke conditions which could be an indication of a fire typically using optical sensors (photoelectric detection) or ionization detection.

Infrared (IR) sensors

Infrared sensor technologies detect infrared radiation that is emitted by objects. Non-contact thermometers make use of these types of sensors as a way of measuring the temperature of an object without having to directly place a probe or sensor on that object. They find use in analyzing the heat signature of electronics and detecting blood flow or blood pressure in patients.

Acceleration sensors

While motion sensors detect movement of an object, acceleration sensors, or accelerometers as they are also known, detect the rate of change of velocity of an object. This change may be due to a free-fall condition, a sudden vibration that is causing movement with speed changes, or rotational motion (a directional change).

8.7. Actuators

An actuator is a machine component or system that moves or controls the mechanism or the system. Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform. Actuators convert an electrical signal into a corresponding physical quantity such as movement, force, sound etc.

8.7.1. Types of Actuators

1. **Servo Motors:**

Servo is a small device that incorporates a two wire DC motor, a gear train, a potentiometer, an integrated circuit, and a shaft (output spine).

2. **Stepper Motors:**

Stepper motors are DC motors that move in discrete steps. They have multiple coils that are organized in groups called “phases”. By energizing each phase in sequence, the motor will rotate, one step at a time. With a computer controlled stepping, you can achieve very precise positioning and/or speed control.

3. **DC Motors (Continuous Rotation Motors):**

Direct Current (DC) motor is the most common actuator used in projects. They are simple, cheap, and easy to use. DC motors convert electrical into mechanical energy. Also, they come in different sizes.

4. **Linear actuator**:

A linear actuator is an actuator that creates motion in a straight line, in contrast to the circular motion of a conventional electric motor. Linear actuators are used in machine tools and industrial machinery, in computer peripherals such as disk drives and printers, in valves and dampers, and in many other places where linear motion is required

5. **Relay:**

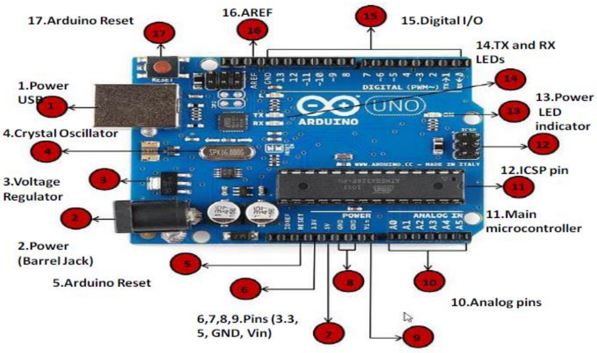
A relay is an electrically operated switch. Many relays use an electromagnet to mechanically operate a switch. The advantage of relays is that it takes a relatively small amount of power to operate the relay coil, but the relay itself can be used to control motors, heaters, lamps or AC circuits which themselves can draw a lot more electrical power

6. **Solenoid:**

A solenoid is simply a specially designed electromagnet. Solenoids are inexpensive, and their use is primarily limited to on-off applications such as latching, locking, and triggering. They are frequently used in home appliances (e.g. washing machine valves), office equipment (e.g. copy machines), automobiles (e.g. door latches and the starter solenoid), pinball machines (e.g., plungers and bumpers), and factory automation

8.8.Computing Components (Arduino, Raspberry Pi)

- Arduino Board: An Arduino is actually a microcontroller based kit.
- It is basically used in communications and in controlling or operating many devices.
- Arduino UNO board is the most popular board in the Arduino board family.
- In addition, it is the best board to get started with electronics and coding.
- Some boards look a bit different from the one given below, but most Arduino's have majority of these components in common.
- It consists of two memories- Program memory and the data memory.
- The code is stored in the flash program memory, whereas the data is stored in the data memory.
- Arduino Uno consists of 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button 1.Power USB 2.Power (Barrel Jack) 3.Voltage Regulator 4.Crystal Oscillator 17.Arduino Reset 5.Arduino Reset 6,7,8,9.Pins (3.3, 5, GND, Vin) 10.Analog pins 11.Main microcontroller 12.ICSP pin 13.Power LED indicator 14.TX and RX LEDs 15.D



Raspberry Pi

- The Raspberry Pi is a very cheap computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins that allow you to control electronic components for physical computing and explore the Internet of Things (IoT).

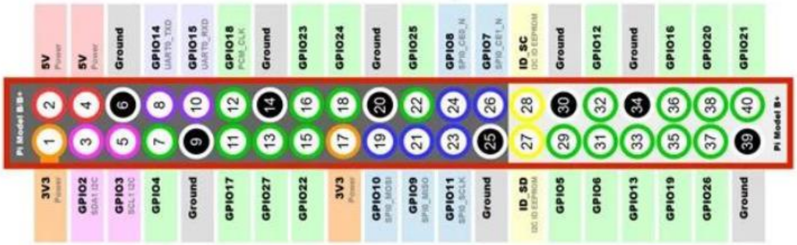
- Raspberry Pi was basically introduced in 2006.
- It is particularly designed for educational use and intended for Python.
- A Raspberry Pi is of small size i.e., of a credit card sized single board computer, which is developed in the United Kingdom(U.K) by a foundation called Raspberry Pi

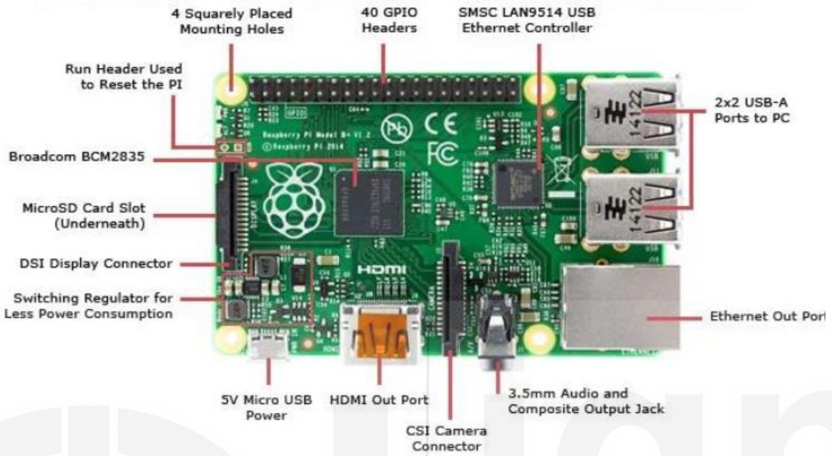
There have been three generations of Raspberry Pis: Pi 1, Pi 2, and Pi 3

- The first generation of Raspberry (Pi 1) was released in the year 2012, that has two types of models namely model A and model B.
- Raspberry Pi can be plugged into a TV, computer monitor, and it uses a standard keyboard and mouse.
- It is user friendly as can be handled by all the age groups.
- It does everything you would expect a desktop computer to do like word-processing, browsing the internet spread sheets, playing games to playing high definition videos.
- All models feature on a broadcom system on a chip (SOC), which includes chip graphics processing unit GPU(a Video Core IV), an ARM compatible and CPU.
- The CPU speed ranges from 700 MHz to 1.2 GHz for the Pi 3 and on board memory range from 256 MB to 1 GB RAM.
- An operating system is stored in the secured digital SD cards and program memory in either the MicroSDHC or SDHC sizes.
- Most boards have one to four USB slots, composite video output, HDMI and a 3.5 mm phone jack for audio. Some models have WiFi and Bluetooth.

- All models feature a Broadcom system on a chip (SoC) with an integrated ARM-compatible central processing unit (CPU) and on-chip graphics processing unit (GPU).
- Processor speed ranges from 700 MHz to 1.4 GHz for the Pi 3 Model B+ or 1.5 GHz for the Pi 4; on-board memory ranges from 256 MB to 1 GB with up to 4 GB available on the Pi 4 random-access memory (RAM).
- Secure Digital (SD) cards in Micro SDHC form factor (SDHC on early models) are used to store the operating system and program memory.
- The boards have one to five USB ports. For video output, HDMI and composite video are supported, with a standard 3.5 mm tip-ring-sleeve jack for audio output.
- Lower-level output is provided by a number of GPIO pins, which support common protocols like I²C. The B-models have an 8P8C Ethernet port and the Pi 3 and Pi Zero W have on-board Wi-Fi and Bluetooth.

GPIO Pinout Diagram




4 Squarely Placed Mounting Holes
40 GPIO Headers
SMSC LAN9514 USB Ethernet Controller
Run Header Used to Reset the PI
2x2 USB-A Ports to PC
Broadcom BCM2835
MicroSD Card Slot (Underneath)
DSI Display Connector
Switching Regulator for Less Power Consumption
Ethernet Out Port
5V Micro USB Power
HDMI Out Port
CSI Camera Connector
3.5mm Audio and Composite Output Jack

8.9.IoT Architecture

The Reference Model introduced in 2014 by Cisco, IBM, and Intel at the 2014 IoT World Forum has as many as seven layers. According to an official press release by Cisco forum host, the architecture aims to *“help educate CIOs, IT departments, and developers on deployment of IoT projects, and accelerate the adoption of IoT.”*

These layers are:

1. The **perception layer** hosting smart things;
2. The **connectivity or transport layer** transferring data from the physical layer to the cloud and vice versa via networks and gateways;
3. The **processing layer** employing IoT platforms to accumulate and manage all data streams; and

4.The **application layer** delivering solutions like analytics, reporting, and device control to end users.

Perception layer: converting analog signals into digital data and vice versa

The initial stage of any IoT system embraces a wide range of “things” or endpoint devices that act as a bridge between the real and digital worlds. They vary in form and size, from tiny silicon chips to large vehicles. By their functions, IoT things can be divided into the following large groups.

Sensors such as probes, gauges, meters, and others. They collect physical parameters like temperature or humidity, turn them into electrical signals, and send them to the IoT system. IoT sensors are typically small and consume little power.

Actuators, translating electrical signals from the IoT system into physical actions.

Machines and devices connected to sensors and actuators or having them as integral parts.

Connectivity layer: enabling data transmission

The second level is in charge of all communications across devices, networks, and cloud services that make up the IoT infrastructure. The connectivity between the physical layer and the cloud is achieved in two ways:

directly, using TCP or UDP/IP stack;

via gateways — hardware or software modules performing translation between different protocols as well as encryption and decryption of IoT data.

The communications between devices and cloud services or gateways involve different networking technologies.

Ethernet connects stationary or fixed IoT devices like security and video cameras, permanently installed industrial equipment, and gaming consoles.

WiFi, the most popular technology of wireless networking, is a great fit for data-intensive IoT solutions that are easy to recharge and operate within a small area. A good example of use is smart home devices connected to the electrical grid.

NFC (Near Field Communication) enables simple and safe data sharing between two devices over a distance of 4 inches (10 cm) or less.

Bluetooth is widely used by wearables for short-range communications. To meet the needs of low-power IoT devices, the Bluetooth Low-Energy (BLE) standard was designed. It transfers only small portions of data and doesn't work for large files.

LPWAN (Low-power Wide-area Network) was created specifically for IoT devices. It provides long-range wireless connectivity on low power consumption with a battery life of 10+ years. Sending data periodically in small portions, the technology meets the requirements of smart cities, smart buildings, and smart agriculture (field monitoring).

ZigBee is a low-power wireless network for carrying small data packages over short distances. The outstanding thing about ZigBee is that it can handle up to 65,000 nodes. Created specifically for home automation, it also works for low-power devices in industrial, scientific, and medical sites.

Cellular networks offer reliable data transfer and nearly global coverage. There are two cellular standards developed specifically for IoT things. LTE-M (Long Term Evolution for Machines) enables devices to communicate directly with the cloud and exchange high volumes of data. NB-IoT or Narrowband IoT uses low-frequency channels to send small data packages.

Edge or fog computing layer: reducing system latency

This level is essential for enabling IoT systems to meet the speed, security, and scale requirements of the 5th generation mobile network or 5G. The new wireless standard promises faster speeds, lower latency, and the ability to handle many more connected devices, than the current 4G standard.

The idea behind edge or fog computing is to process and store information as early and as close to its sources as possible. This approach allows for analyzing and transforming high volumes of real-time data locally, at the edge of the networks. Thus, you save the time and other resources that otherwise would be needed to send all data to cloud services. The result is reduced system latency that leads to real-time responses and enhanced performance.

Processing layer: making raw data useful

The processing layer accumulates, stores, and processes data that comes from the previous layer. All these tasks are commonly handled via IoT platforms and include two major stages.

Data accumulation stage

The real-time data is captured via an API and put at rest to meet the requirements of non-real-time applications. The data accumulation component stage works as a transit hub between event-based data generation and query-based data consumption.

Among other things, the stage defines whether data is relevant to the business requirements and where it should be placed. It saves data to a wide range of storage solutions, from data lakes capable of holding unstructured data like images and video streams to event stores and telemetry databases. The total goal is to sort out a large amount of diverse data and store it in the most efficient way.

Data abstraction stage

Here, data preparation is finalized so that consumer applications can use it to generate insights. The entire process involves the following steps:

combining data from different sources, both IoT and non-IoT, including ERM, ERP, and CRM systems; reconciling multiple data formats; and aggregating data in one place or making it accessible regardless of location through data virtualization.

Similarly, data collected at the application layer is reformatted here for sending to the physical level so that devices can “understand” it.

Together, the data accumulation and abstraction stages veil details of the hardware, enhancing the interoperability of smart devices. What’s more, they let software developers focus on solving particular business tasks — rather than on delving into the specifications of devices from different vendors.

Application layer: addressing business requirements

At this layer, information is analyzed by software to give answers to key business questions. There are hundreds of IoT applications that vary in complexity and function, using different technology stacks and operating systems. Some examples are:

device monitoring and control software, mobile apps for simple interactions, business intelligence services, and analytic solutions using machine learning.

Currently, applications can be built right on top of IoT platforms that offer software development infrastructure with ready-to-use instruments for data mining, advanced analytics, and data visualization. Otherwise, IoT applications use APIs to integrate with middleware.

Business layer: Implementing data-driven solutions

The information generated at the previous layers brings value if only it results in problem-solving solution and achieving business goals. New data must initiate collaboration between stakeholders who in turn introduce new processes to enhance productivity.

The decision-making usually involves more than one person working with more than one software solution. For this reason, the business layer is defined as a separate stage, higher than a single application layer.

Security layer: preventing data breaches

It goes without saying that there should be a security layer covering all the above-mentioned layers. IoT security is a broad topic worthy of a separate article. Here we’ll only point out the basic features of the safe architecture across different levels.

Device security. Modern manufacturers of IoT devices typically integrate security features both in the hardware and firmware installed on it. This includes embedded TPM (Trusted Platform Module) chips with cryptographic keys for authentication and protection of endpoint devices;

a secure boot process that prevents unauthorized code from running on a powered-up device; updating security patches on a regular basis; and physical protection like metal shields to block physical access to the device.

Connection security. Whether data is being sent over devices, networks, or applications, it should be encrypted. Otherwise, sensitive information can be read by anybody who intercepts information in transit. IoT-centric messaging protocols like MQTT, AMQP, and DDS may use standard Transport Layer Security (TSL) cryptographic protocol to ensure end-to-end data protection.

Cloud security. Data at rest stored in the cloud must be encrypted as well to mitigate risks of exposing sensitive information to intruders. Cloud security also involves authentication and authorization mechanisms to limit access to the IoT applications. Another important security method is device identity management to verify the device’s credibility before allowing it to connect to the cloud.

The good news is that IoT solutions from large providers like Microsoft, AWS, or Cisco come with pre-built protection measures including end-to-end data encryption, device authentication, and access control. However, it always pays to ensure that security is tight at all levels, from the tiniest devices to complex analytical systems.

Applications of IoT

1. **IoT Wearables**

Wearable technology is a hallmark of IoT applications and probably is one of the earliest industries to have deployed the IoT at its service. We happen to see Fit Bits, heart rate monitors and smart watches everywhere these days.

One of the lesser-known wearables includes the Guardian glucose monitoring device. The device is developed to aid people suffering from diabetes. It detects glucose levels in the body, using a tiny electrode called glucose sensor placed under the skin and relays the information via Radio Frequency to a monitoring device.

2. IoT Applications – Smart Home Applications

When we talk about IoT Applications, Smart Homes are probably the first thing that we think of. The best example I can think of here is *Jarvis*, the AI home automation employed by Mark Zuckerberg. There is also Allen Pan's Home Automation System where functions in the house are actuated by use of a string of musical notes

3. IoT Applications – Health Care

IoT applications can turn reactive medical-based systems into proactive wellness-based systems.

The resources that current medical research uses, lack critical real-world information. It mostly uses leftover data, controlled environments, and volunteers for medical examination. IoT opens ways to a sea of valuable data through analysis, real-time field data, and testing.

The Internet of Things also improves the current devices in power, precision, and availability. IoT focuses on creating systems rather than just equipment

4. IoT Applications – Smart Cities

By now I assume, most of you must have heard about the term **Smart City**. The hypothesis of the optimized traffic system I mentioned earlier, is one of the many aspects that constitute a smart city.

The thing about the smart city concept is that it's very specific to a city. The problems faced in Mumbai are very different than those in Delhi. The problems in Hong Kong are different from New York. Even global issues, like finite clean drinking water, deteriorating air quality and increasing urban density, occur in different intensities across cities. Hence, they affect each city differently.

5. IoT Applications – Agriculture

Statistics estimate the ever-growing world population to reach nearly 10 billion by the year 2050. To feed such a massive population one needs to marry agriculture to technology and obtain best results. There are numerous possibilities in this field. One of them is the **Smart Greenhouse**.

A greenhouse farming technique enhances the yield of crops by controlling environmental parameters. However, manual handling results in production loss, energy loss, and labor cost, making the process less effective.

6. IoT Applications – Industrial Automation

This is one of the fields where both faster developments, as well as the quality of products, are the critical factors for a higher Return on Investment. With IoT Applications, one could even re-engineer products and their packaging to deliver better performance in both cost and customer experience. IoT here can prove to be game changing with solutions for all the following domains in its arsenal.

Factory Digitalization
Product flow Monitoring
Inventory Management
Safety and Security
Quality Control
Packaging optimization
Logistics and Supply Chain Optimization

8.10. Challenges of IoT

The biggest challenges for IoT adoption include:

- Security Challenges
- Regulation Challenges
- Compatibility Challenges
- Bandwidth Challenges
- Customer Expectation Challenges

Security Challenges:

Rapid advances in both technology and the complexity of cyber-attacks have meant that the risk of security breaches has never been higher. There is an increased responsibility for software developers to create the most secure applications possible to defend against this threat as IoT devices are often seen as easy targets by hackers.

Regulation Challenges

We've already touched on how GDPR has impacted the IoT industry, however, as the industry is still relatively new and young, it generally lacks specific regulation and oversight, which is required to ensure that all devices are produced with a suitable level of protection and security.

.

Compatibility Challenges

At the core of the IoT concept, all devices must be able to connect and communicate with each other for data to be transferred.

The IoT industry currently lacks any compatibility standards, meaning that many devices could all run on different standards resulting in difficulties communicating with one another effectively.

Bandwidth Challenges

Perhaps at no surprise, devices and applications that rely on the ability to communicate with each other constantly to work effectively tend to use a lot of data at once, leading to bandwidth constraints for those using many devices at once.

Combine this with existing demands for data and broadband in the typical house, and you can quickly see how data and bandwidth limitations can be a challenge.

Customer Expectation Challenges

Arguably the biggest hurdle for the industry relates to customer perception. For anything new to be adopted by the masses, it has to be trusted completely.

For the IoT industry, this is a continuously evolving challenge as it relies on the ability to actively combat security threats and reassure the general consumer market that the devices are both safe to use and secure to hold vast quantities of sensitive data

UNIT 9 IoT NETWORKING AND CONNECTIVITY TECHNOLOGIES

9.1 INTRODUCTION

Machine-to-Machine or M2M is a technology that allows connectivity between network devices. It allows tapping of sensor data and transmitting it over a public network. IoT technology, on the other hand, expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. It allows users to create high performance, fast and flexible networks that can connect a variety of devices.

9.2 OBJECTIVES

After going through this unit, you should be able to:

- Know about the M2M and IoT technology
- Know about the components required for IoT implementation
- Know about gateway prefix allotment & impact of mobility
- Know about various identification and data protocols
- Know about various connectivity technologies

9.3 M2M AND IoT TECHNOLOGY

Machine-to-Machine or M2M is a technology that allows connectivity between network devices. This point to point connectivity is established to transfer information over public networks like ethernet or cellular networks without human intervention. Its main purpose is to tap sensor data and transmit it over a public network. The use of public networks makes it cost efficient. It has many applications in the sectors like health care, insurance, business etc.

Various components that make up an M2M system are - sensors, RFID (Radio Frequency Identification) , Wi-Fi or cellular network, and a computing software which helps networking devices to interpret data and decision making. These M2M applications can translate data which in turn can trigger automated actions.Various benefits offered by M2M are -

1. It reduces cost by making use of public network and minimizing downtime
2. Increase revenue by identifying new business opportunities
3. Increase customer satisfaction by timely servicing equipment and regularly monitoring.

M2M Applications

Sensor telemetry is one of the first application of M2M communication. It has been used since the last century for transmitting operational data. Earlier people used telephone lines, then radio waves, to transmit measurements factors like- temperature, pressure etc for remote monitoring. Another example of M2M communication is ATM. ATM machine routes information regarding request for transaction to appropriate bank. The bank in turn through its system approves it and allows transactions to complete. It also has applications in supply chain management (SCM), warehouse management systems (WMS), Utility companies, etc. Fig 1 shows various applications of M2M.

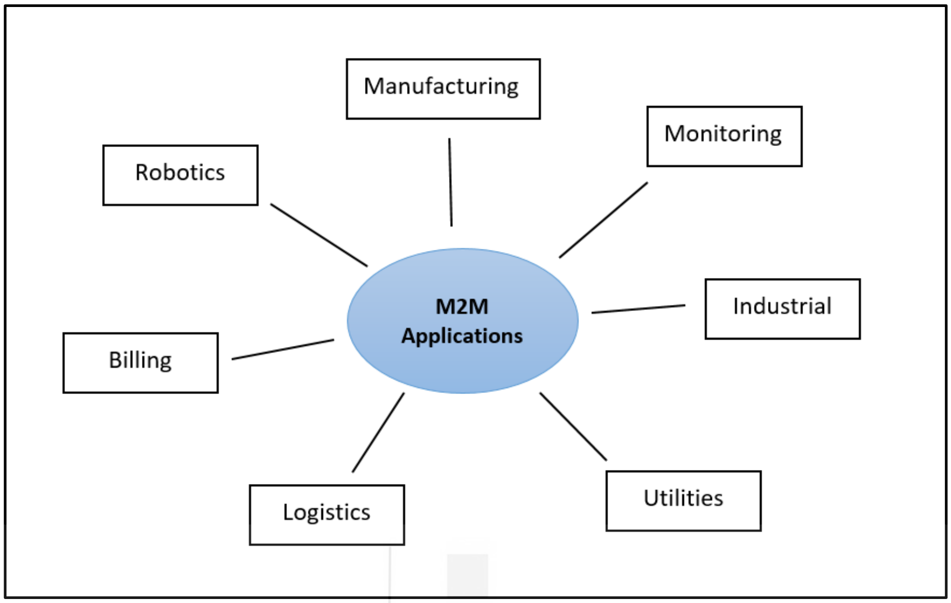


Fig 1. Applications of M2M

Internet of Things (IoT)

Internet of Things or IoT, is a technology that has evolved from M2M by increasing the capabilities at both consumers and enterprise level. It expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. It allows users to create high performance, fast and flexible networks that can connect a variety of devices. Table 1 summarizes the differences between M2M and IoT devices.

IoT is a network of physical objects , called “Things” , embedded with hardware like - sensors or actuators or software, for exchanging data with other devices over the internet. With the help of this technology, it is possible to connect any kind of device like simple household objects example- kitchen appliances, baby monitors, ACs, TVs, etc to other objects like- cars, traffic lights, web camera, etc. Connecting these objects to the internet through embedded devices, allows seamless communication between things, processes or people. Some of the applications of IoT devices are – smart home voice assistant Alexa, smart traffic light system.

IoT devices when connected to cloud platforms, can provide a huge and wide variety of industrial or business applications. As the number of IoT devices are increasing, the problem of storing, accessing and processing is also emerging. IoT when used with Cloud technology provides solutions to these problems due to huge infrastructure provided by cloud providers.

Table 1. Difference between M2M and IoT devices

M2M – Machine 2 Machine	**IoT – Internet of Things**
Point to point connection establishment	Devices are connected through the network and also supports connecting to global cloud networks.
Limited amount of intelligence	Decision making is enabled
Makes use of internet protocols like- HTTP, FTP, etc.	Makes use of traditional communication protocols
Generally may not rely on internet connection	Generally Rely on internet connection
Less scalable	Highly scalable

9.4COMPONENTS OF IoT IMPLEMENTATION

IoT systems can be implemented by four components.

1. Sensors
   Sensors are devices that are capable of collecting data from the environment. There are various types of sensors available –temperature sensors, pressure sensors, RFID tags, light intensity detectors, electromagnetic sensors, etc.

2. Network
   Data collected from sensors are passed over the network for computations to the cloud or processing nodes. Depending upon the scale, they may be connected over LAN, MAN or WAN. They can also be connected through wireless networks like- Bluetooth, ZigBee, Wi-Fi, etc.

3. Analytics
   The process of generating useful insights from the data collected by sensors is called analytics. Analytics when performed in real time, can have numerous applications and can make the IoT system efficient.

4. Action

Information obtained after analytics must be either passed to the user using some user interface, messages, alerts, etc; or may also trigger some actions with the help of actuators. Actuators are the devices that perform some action depending on the command given to them over the network.

Fig 2 shows implementation of IoT. Data captured by sensors are passed on to the cloud servers over the internet via gateways. Cloud servers in turn perform analytics and pass on the decisions or commands to actuators.

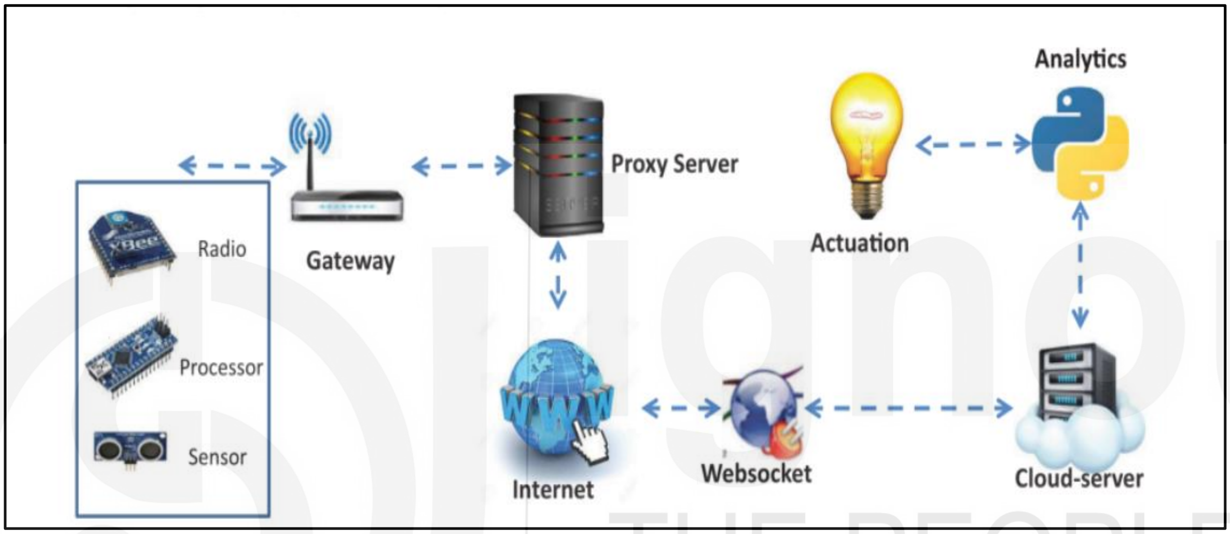


Fig 2:IoT implementation
(Source: Reference 1)

Check your Progress 1

1. What is IoT technology?
2. State differences between M2M and IoT technology.
3. What are the various components involved in implementation of IoT?

9.5 GATEWAY PREFIX ALLOTMENT

Gateways are networking devices that connect IoT devices like sensors or controllers to Cloud. In other ways we can say that data generated by IoT devices are transferred to Cloud servers through IoT gateways.

The number of IoT devices is increasing at an exponential rate. These IoT devices are connected in a LAN or a WAN. A number of IoT devices within a building, communicating to a gateway installed in the same building over a wi-fi connection can be called an IoT LAN. Geographically distributed LAN segments are interconnected and connected to the internet via gateways to form IoT WAN. Devices connected within LAN have unique IP addresses but may have addresses the same as devices of another LAN .

Gateways connect IoT LANs and WANs together. It is responsible for forwarding packets between them on the IP layer. Since a large number of devices are connected, address space needs to be conserved. Each connected device needs a unique address. IP addresses allocated to devices within a gateway's jurisdiction are valid only in its domain. Same addresses may be allocated in another gateway's domain. Hence to maintain uniqueness, each gateway is assigned a unique network prefix. It is used for global identification of gateways. This unique identifier removes the need of allocating a unique IP address to each and every device connected to the network, hence saves a lot of address space.

Gateway prefix allotment is shown in fig 3. Here two gateway domains are shown. Both of them are connected to the internet via router. This router has its own address space and allows connectivity to the internet. This router assigns a unique gateway prefix to both the gateways. Hence packets are forwarded from gateways to the internet via routers.

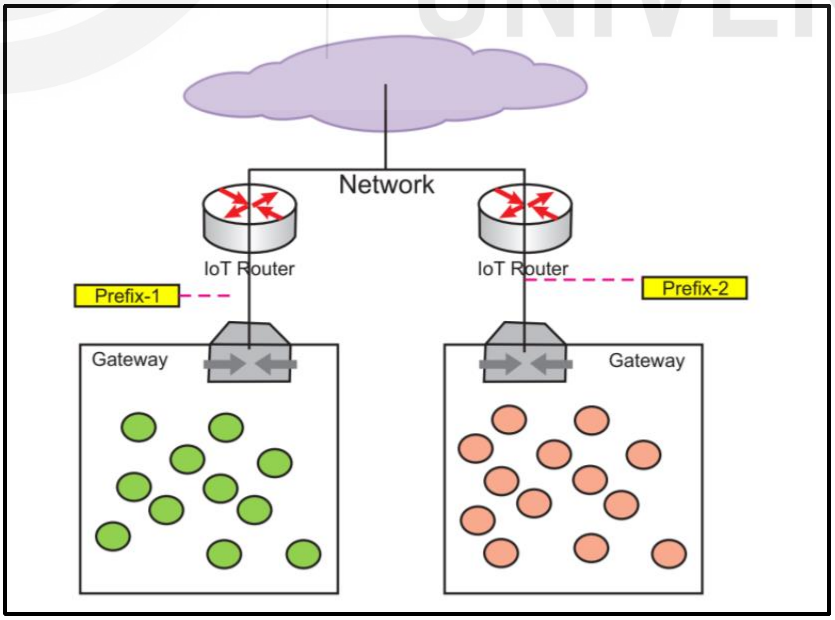


Fig 3: Gateway prefix allotment
(Source: Reference 1)

9.6 IMPACT OF MOBILITY ON ADDRESSING

When an IoT device moves from one location to another in a network, its address is affected. Network prefix allocated to gateways change due to mobility. WAN addresses allocated to devices through gateways changes without affecting IoT LAN addresses. This is possible because addresses allocated within a domain of gateway are unique. It is not affected by mobility of devices. These unique local addresses (ULA) are maintained independent of global addresses. For giving internet access to these ULAs, they are connected to application layer proxy which routes them globally.

Gateways are attached to a remote anchor point by using protocols like IPv6. These remote anchor points are immune to changes of network prefix. It is also possible for the nodes in a network to establish direct connection with remote anchor points to access the internet directly using tunneling. Fig 4 shows remote anchor points having access to gateways.

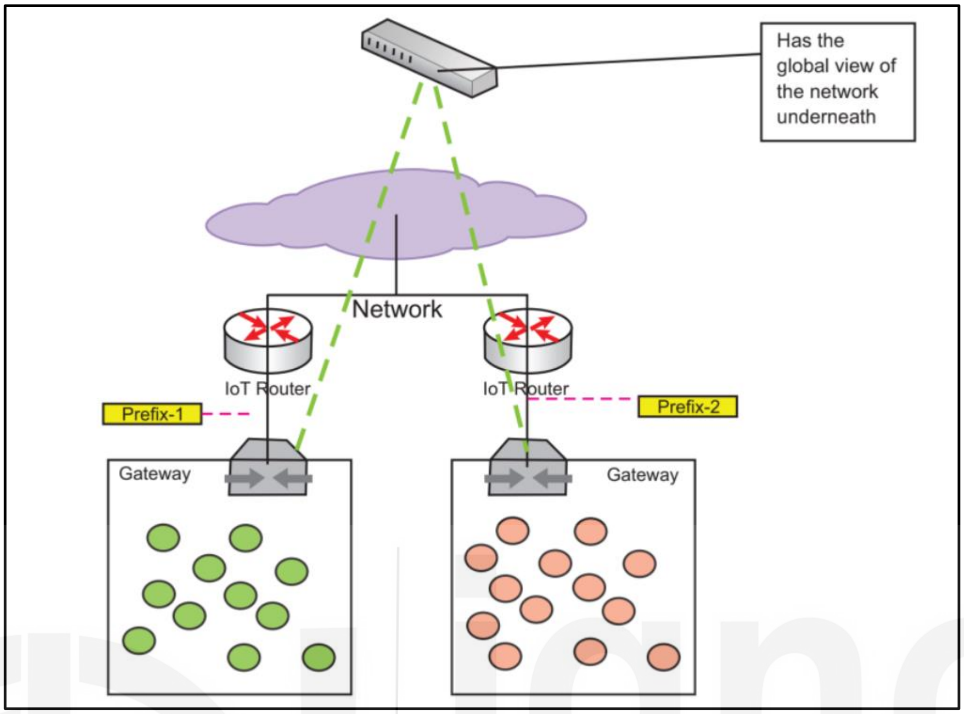


Fig 4: Remote anchor point
(Source: Reference 1)

9.7 MULTIHOMING

The practice of connecting a host to more than one network is called Multihoming. This can increase reliability and performance. Various ways to performmultihoming are –

1. Host multihoming
   In this type of multihoming, a single host can be connected to two or more networks. For example a computer connected to both a local network and awi-fi network.

2. Classical multihoming
   In this type of multihoming, a single network is connected to multiple providers. Edge router communicates with providers using dynamic routing protocols. This protocol can recognize failures and reconfigure routing tables without hosts being aware of it. It requires address space recognized by all providers, hence it is costly.

9.8 IoT IDENTIFICATION AND DATA PROTOCOLS

IoT devices are diverse in their architecture and its use cases can scale from single device deployment to massive cross-platform deployment. There are various types of communication protocols that allow communication between these devices. Some of the protocols are given below.

IPv4

Internet Protocol is a network layer protocol version 4 used to provide addresses to hosts in a network. It is a widely used communication protocol for different kinds of networks. It is a connectionless protocol that makes use of packet switching technology. It is used to give a 32 bit address to a host. It is divided into five classes – A, B, C, D, and E. It can provide upto 4.3 billion addresses only which is not sufficient for an IoT device. It allows data to be encrypted but does not limit access to data hosted on the network.

IPV6

As the total number of addresses provided by IPv4 are not sufficient specially for IoT devices, Internet protocol version 6 or IPv6 is introduced. It is an upgraded version of IPv4. It uses 128 bits to address a host hence anticipates future growth and provides relief from shortage of network addresses. It gives better performance than IPv4. It also ensures privacy and data integrity. It is automatically configured and has built-in support for authentication. Some of the differences between IPv4 and IPv6 are shown in table 2.

Table 2. Differences between IPv4 and IPv6

IPv4	IPv6
Its length is 32 bits	Its length is 128 bits
Possible number of addresses are 2^{32}	Possible number of addresses are 2^{128}
It is represented in dotted decimal notation	It is represented in hexadecimal notation
IPsec is optional	IPsec is compulsory
It supports manual or DHCP configuration	It supports auto-configuration

It supports broadcasting	It supports multicasting

MQTT

Message queuing telemetry transport (MQTT) is a widely used light-weight messaging protocol based on subscription. It is used in conjunction with TCP/IP protocol. It is designed for battery powered devices. Its model is based on Subscriber, Publisher and Broker. Publishers are light weight sensors and subscribers are applications which will receive data from publishers. Subscribers need to subscribe to a topic. Messages updated in a topic are distributed by brokers. Publisher collects the data and sends it to the subscriber through a broker. Broker after receiving messages, filtering and making decisions, sends messages to the subscribers. Brokers also ensure security by authorizing subscribers and publishers. Fig 5 shows the working of MQTT.

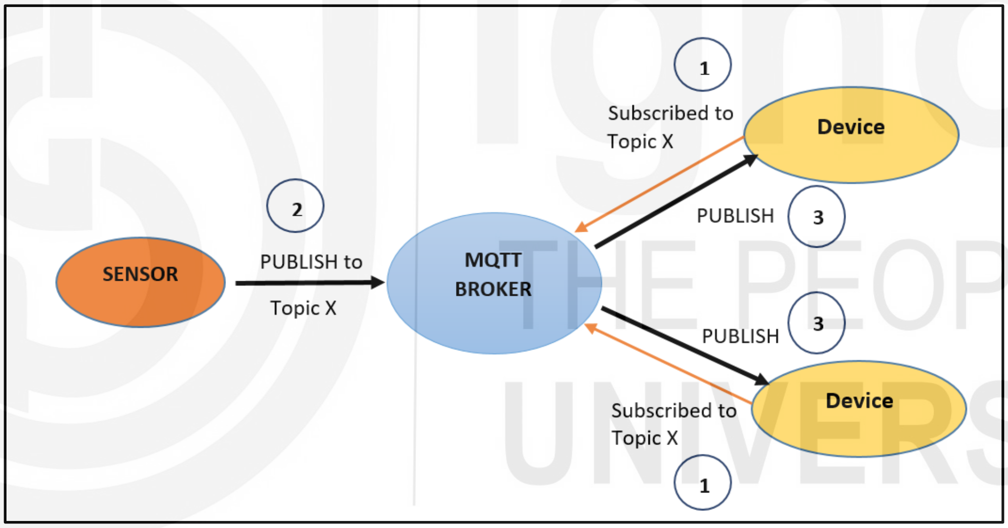


Fig 5: Working of MQTT

CoAP

Constrained Application Protocol (CoAP) is a web transfer protocol used to translate the HTTP model so as to be used with restrictive devices and network environments.It is used for low powered devices. It allows low power sensors to interact with RESTful services. It makes use of UDP for establishing communication between endpoints. It allows data to be transmitted to multiple hosts using low bandwidth.

XMPP

Extensible messaging and presence protocol (XMPP) enables real time exchange of extensible data between network entities. It is a communication protocol based on XML i.e. extensible markup language. It is an open standard hence anyone can implement these services. It also supports M2M communication across a variety of networks. It can be used for instant messaging, multi-party chat, video calls, etc.

AMQP

Advanced message queuing protocol i.e AMQP is an application layer message oriented protocol. It is open standard, efficient, multi-channel, portable and secure. This is fast and also guarantees delivery along with acknowledgement of received messages. It can be used for both point-to-point and publish-subscribe messaging. It is used for messaging in client-server environments. It also supports a multi-client environment and helps servers to handle requests faster.

Need to elaborate more on Protocols?

9.8 CONNECTIVITY TECHNOLOGIES

IoT devices need to be connected in order to work. Various technologies used to establish connections between devices are discussed in this section.

IEEE 802.15.4

It is an IEEE standard protocol used to establish wireless personal area networks (WPAN). It is used for providing low cost, low speed, ubiquitous networks between devices. It is also known as Low-Rate wireless Personal Area Network (LR-WPAN) standard. It makes use of the first two layers (Physical and MAC layers) of the network stack and operates in ISM band. These standards are also used with communication protocols of higher levels like- ZigBee, 6LoWPAN, etc.

6LoWpan

IPV6 over low power wireless personal area network, is a standard for wireless communication. It was the first standard created for IoT. It allows small, limited processing capabilities and low power IoT devices to have direct connectivity with IP based servers on the internet. It also allows IPV6 packets to be transmitted over IEEE 802.15.4 wireless network.

ZigBee

It is a wireless technology based on IEEE 802.15.4 used to address needs of low-power and low-cost IoT devices. It is used to create low cost, low power, low data rate wireless ad-hoc networks. It is resistant to unauthorized reading and communication errors but provides low throughput. It is easy to install, implement and supports a large number of nodes to be connected. It can be used for short range communications only.

NFC

Near Field Communication (NFC) is a protocol used for short distance communication between devices. It is based on RFID technology but has a lower transmission range (of about 10 cm). It is used for identification of documents or objects. It allows contact less transmission of data. It has shorter setup time than Bluetooth and provides better security.

Bluetooth

It is one of the widely used types of wireless PAN used for short range transmission of data. It makes use of short range radio frequency. It provides data rate of appx 2.1 Mbps and operates at 2.45GHz. It is capable of low cost and low power transmission for short distances. Its initial version 1.0 supported upto 732kpbs speed. Its latest version is 5.2 which can work upto 400m range with 2 Mbps data rate.

Z-Wave

It is one of the standards available for wireless networks. It is interoperable and uses low powered radio frequency communication. It is used for connecting to smart devices by consuming low power. These Z-waves devices allow IoT devices to be controlled over the internet. It is generally used for applications like home automation . It supports data rate of upto 100kbps. It also supports encryption and multi-channel.

RFID

Radio frequency identification (RFID) are electronics devices consisting of an antenna and a small chip. This chip is generally capable of carrying data upto 2000 bytes. It is used to give unique identification to an object. Its system is composed of reading device and RFID tags. RFID tags are used to store data and identification information, which is then attached to the object to be tracked. The reader is used to track presence of RFID tag when the object passes through it.

Check your Progress 2

1. What is Gateway prefix ? Why it is needed.
2. State differences between IPv4 and IPv6.
3. Explain any three connectivity technologies.

Need to elaborate more on the above technologies?

9.9 SUMMARY

In this unit M2M and IoTtechnologies are discussed in detail. Machine-to-Machine is a technology that allows connectivity between networking devices. IoT technology expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. In order to implement IoT, components involved are – sensors, network, analytics and actions (actuators). Some of the existing IoT identification and data protocols are IPv4, IPv6, MQTT, XMPP, etc. Existing connectivity technologies used for connecting devices are – Bluetooth, Zigbee, 802.15.4, RFID, etc.

References

1. “Internet of Things”, Dr.JeevaJose , 2018, Khanna Book Publishing Co. (P) LTD. ISBN: 978-93-86173-59-1.

Solutions to Check your Progress 1

1. IoT is a network of physical objects , called “Things” , embedded with hardware like - sensors or actuators or software, for exchanging data with other devices over the internet. With the help of this technology, it is possible to connect any kind of device like simple household objects example- kitchen appliances, baby monitors, ACs, TVs, etc.

2. The various differences between IoT and M2M are –

M2M	IoT
Machine 2 Machine	Internet of Things
Point to point connection establishment	Devices are connected through the network and also supports connecting to global cloud networks.
Limited amount of intelligence	Decision making is enabled
Makes use of internet protocols like- HTTP, FTP, etc.	Makes use of traditional communication protocols
Generally may not rely on internet connection	Generally Rely on internet connection
Less scalable	Highly scalable

3. The components involved in the implementation of IoT are –
   a) Sensors - devices that are capable of collecting data from the environment. There are various types of sensors available –temperature sensors, pressure sensors, RFID tags, light intensity detectors, electromagnetic sensors, etc.
   b) Network - Data collected from sensors are passed over the network for computations to the cloud or processing nodes.
   c) Analytics - The process of generating useful insights from the data collected by sensors is called analytics.

a) Action - Information obtained after analytics must be either passed to the user using some user interface, messages, alerts, etc; or may also trigger some actions with the help of actuators.

Solutions to Check your Progress 2

1. Gateways connect IoT LANs and WANs together. It is responsible for forwarding packets between them on the IP layer. Since a large number of devices are connected, address space needs to be conserved. Each connected device needs a unique address. IP addresses allocated to devices within a gateway's jurisdiction are valid only in its domain. Same addresses may be allocated in another gateway's domain. Hence to maintain uniqueness, each gateway is assigned a unique network prefix. It is used for global identification of gateways.

2. Both IPv4 and IPv6 are network layer protocols. Some of the differences are –

IPv4	IPv6
Its length is 32 bits	Its length is 128 bits
Possible number of addresses are 2^{32}	Possible number of addresses are 2^{128}
It is represented in dotted decimal notation	It is represented in hexadecimal notation
IPsec is optional	IPsec is compulsory
It supports manual or DHCP configuration	It supports auto-configuration

3. V
   arious connectivity technologies are –

   a) IEEE 802.15.4 - It is an IEEE standard protocol used to establish wireless personal area networks (WPAN). It is used for providing low cost, low speed, ubiquitous networks between devices.

   b) 6LoWpan - IPV6 over low power wireless personal area network, is a standard for wireless communication. It was the first standard created for IoT. It allows small, limited processing capabilities and low power IoT devices to have direct connectivity with IP based servers on the internet.

c) RFID - Radio frequency identification (RFID) are electronics devices consisting of an antenna and a small chip. This chip is generally capable of carrying data upto 2000 bytes. It is used to give unique identification to an object.