**Wireless Networks and IOT Devices**

Kadgonda A Patil1

1Assistant Professor, Department of Electronics and Computer Engineering, SITCOE, Yadrav, Maharashtra

[Email-sachinkupade@gmail.com](mailto:Email-sachinkupade@gmail.com)

**Wi-Fi:-**

Wi-Fi is the name given to some varieties of wireless local area networks (WLAN) that make use of the 802.11 family of specifications. Peer-to-peer Wi-Fi Direct is one such protocol that enables data transfer between authorized devices without the need for a wireless router or an internet connection. Products bear the trademark "Wi-Fi CERTIFIED," which is a registered trademark of the Wi-Fi Alliance, after passing certification for application-specific protocols, security, and interoperability.

**How is WiFi operated?**

With the usage of a Wi-Fi range extender, a Wi-Fi network can wirelessly send data across a local area network (LAN) by using radio waves. Data delivered by radio waves is translated by a computer using a wireless adaptor. These waves are not the same as those produced by FM radios, for instance, whose frequency is expressed in megahertz (MHz). The frequency at which Wi-Fi signals are carried range from 2.5 to 5 gigahertz (GHz). Subsequently, the signal is routed from the adapter via a router and transferred to the internet.

**Hotspots: what are they?**

Wi-Fi is frequently utilized as a substitute for wired LANs in homes, offices, organizations, and educational settings. Numerous hotels, fast-food restaurants, and airports provide public Wi-Fi networks. We refer to these places as hotspots. While many offer access for a daily or hourly fee, some are free. A hot zone is an area that is connected to other hotspots and network access points. Using their cellular network connections, modern smartphones and tablets can also function as Wi-Fi hotspots, offering computers and other devices wireless internet connectivity. In residences, workplaces, institutions of higher learning, and other locations, wired LANs are being replaced with wireless networks. Public Wi-Fi is available at many hotels, fast-food restaurants, and airports. These locations are known as hotspots. Some are free, while many charge a daily or hourly cost for access. An area with connections to other hotspots and network access points is called a hot zone. Modern smartphones and tablets can serve as Wi-Fi hotspots, providing wireless internet connectivity to computers and other devices, by utilizing their cellular network connections. Computers should come with wireless adapters in order to connect to Wi-Fi hotspots. Laptops and portable electronics like tablets and phones have these. If your computer doesn't come with one of these adapters, you can buy one that fits into a USB port or PCI slot. After that, your computer ought to be able to find nearby Wi-Fi networks on its own. These networks can be either open or protected, with the latter requiring the entry of a Wi-Fi password in order to connect. Unauthorized people may be able to access a Wi-Fi network and use it as a free internet connection if it is not sufficiently secured. War driving is the process of identifying and taking advantage of wireless LANs that have security flaws. War chalking is an identifiable symbology that has developed. Virtual private networks (VPNs), Internet Protocol Security (IPsec), Wi-Fi Protected Access (WPA), the more recent Wired Equivalent Privacy (WEP) encryption standard, and other security measures should be implemented by any organization that uses a wireless local area network (LAN). The Wi-Fi Alliance coined the acronym Wi-Fi as a play on Hi-Fi, which stands for high fidelity and describes high-quality music reproduction. Similarly, Wi-Fi is sometimes used as a shorthand for wireless fidelity. However, according to the Wi-Fi Alliance, Wi-Fi is not a contraction. The Alliance briefly referred to Wi-Fi as "The standard for wireless fidelity," which may have caused confusion. Initially, only 802.11b-compliant items could earn the Wi-Fi certification. These days, any product that adheres to the 802.11 standard can use Wi-Fi. The 802.11 family of wireless network standards, which includes the 802.11 specifications, is a dynamic group of standards. The "flavor" of a Wi-Fi network refers to the unique guidelines that it runs under. Wi-Fi is a networking technology that uses radio waves to provide fast data transfer over short distances. Wi-Fi technology originated from the 1985 decision made by the U.S. Federal Communications Commission to let anyone to utilize the radio spectrum bands of 900 megahertz (MHz), 2.4 gigahertz (GHz), and 5.8 GHz without a license. Technology companies began building wireless networks and devices to take advantage of the newly available radio spectrum. But because it was rare for gadgets made by different manufacturers to work together, the movement remained dispersed. The absence of a single wireless standard was the cause of this. After some time, a group of well-known businesses created the 802.11 standard, which was approved in 1997 by the Institute of Electrical and Electronics Engineers (IEEE). An international nonprofit group known as the Wireless. (Wi-Fi is not a contraction for "wireless fidelity"; a marketing firm hired by WECA came up with the moniker, which was picked for its aesthetically attractive sound and resemblance to "hi-fi" [high-fidelity].) Later IEEE Wi-Fi standards have made it possible to use more bandwidth. Wi-Fi 6 (or 802.11ax) was introduced in 2019 and offers a maximum theoretical speed of 9.6 gigabits per second (Gbps), according to the Wi-Fi Alliance. The maximum data transmission rate allowed by the original 802.11 standard was 2 megabits per second (Mbps). The IEEE Wi-Fi standards split the available radio bands into several channels. Because these channels overlap in frequency, Wi-Fi uses channels that are widely apart. The "spread spectrum" method used by Wi-Fi divides a signal into multiple frequencies and sends it over each of these channels. Thanks to spread spectrum technology, multiple devices can share a single Wi-Fi transmitter and the signal can be provided at a lower power per frequency. Wi-Fi signals are usually transmitted over short distances (less than 100 meters, or 330 feet) in indoor environments, which can lead to multipath interference. This occurs when the signal reflects off of walls, furniture, and other obstructions, arriving at multiple times. By combining three distinct signal transmission methods, Wi-Fi lowers multipath interference. The number of people using WiFi has been steadily rising. Local area networks, or LANs, are becoming more common in homes and businesses as a result of Wi-Fi's ability to do away with the need for cables and cabling. Wi-Fi can also be used to provide wireless broadband Internet access for many modern items, including laptops, cell phones, tablet PCs, and electronic game consoles. Internet access can be gained by Wi-Fi-enabled devices when they are close to "hotspots," or places having Wi-Fi connections. Hotspots are standard since so many public places have Wi-Fi, such as hotels, bookstores, coffee shops, and airports. In some cities, free Wi-Fi networks have been installed throughout.

**Wi-Max**

Wi-Max stands for Worldwide Interoperability for Microwave Access. IEEE 802.16 serves as the technology's cornerstone. It is used to provide quicker data rates and greater coverage. Metropolitan Area Networking is the name of the technology that powers it (MAN). Its range is 50 kilometers. It can operate non-line-of-sight and has a potential throughput of 70 Mbps. This technology is practical, fast, and reasonably priced. Wi-MAX is one of the most widely used broadband wireless technologies on the market today. It is projected that Wi-MAX systems will offer household and business users affordable broadband access services. In order to provide internet access to users, Wi-Max is simply a standardized wireless Ethernet version designed to replace wire technologies like DSL, cable modems, and T1/E1 lines. To be more precise, Wi-MAX is an industry trade group that was founded by leading manufacturers of telecom, equipment, and componentry to support and certify the interoperability and compatibility of broadband wireless access equipment that conforms with IEEE 802.16 and ETSI HIPERMAN standards. Wi-MAX would work similarly to Wi-Fi but faster over longer distances and for more users. Wi-MAX is able to operate in areas that are difficult for wired infrastructure to access and can get beyond the physical limitations of typical wired infrastructure. Wi-MAX was created in April 2001 while waiting for the initial IEEE 802.16 specifications for frequencies in the range of 10 to 66 GHz to be released. Wi-MAX is to 802.16 as the Wi-Fi Alliance is to 802.11.

• Wi-MAX, which stands for Worldwide Interoperability for Microwave Access, is based on Wireless MAN technology.

• A wireless technology intended to offer long-range IP-centric services.

• A wireless platform that is scalable and may be used to create alternative and complementary broadband networks.

• A certification proving that a piece of gear complies with IEEE 802.16 requirements or something similar. The IEEE 802.16 Working Group's specifications address two categories of usage models: a model of fixed usage (IEEE 802.16-2004). A portable usage model (IEEE 802.16e).

**802.16a: What is it?**

Given the simplicity of the name, Wi-MAX is often misused to refer to the 802.16 standards and technology itself, despite the fact that it actually only refers solely to systems that meet specific compliance requirements set forth by the Wi-MAX Forum. Broadband wireless access for fixed, portable, and mobile devices can be provided via a wireless metropolitan area network (MAN) that operates at frequencies between 2 and 11 GHz and adheres to the 802.16a specification. It can be used to provide Internet access to 802.11 hot spots, provide wireless last-mile broadband connection as an alternative to cable or DSL, and provide connectivity on campuses.

**Wi-Max Range and Speed**

Wi-MAX is expected to initially offer up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the exact technical configuration chosen. This is enough to power hundreds of companies with T-1 speed connectivity and thousands of residences with DSL speed connectivity. Wi-MAX is capable of handling video, audio, and Internet traffic. Wi-Max was developed to provide wireless broadband access to buildings, either as a stand-alone solution in underserved rural or sparsely inhabited areas, or as a replacement for existing wired networks. It can also be used to link WLAN hotspots to the Internet.

Broadband connectivity for mobile devices is one of Wi-MAX's other objectives. An approximate 15 Mbps capacity is expected for a 3 km cell coverage area, albeit it would not be as fast as in these stationary applications. Wi-MAX gives users the freedom to ditch their existing internet service provider and gain broadband internet connection from almost anywhere in a Metro Zone. The following spectrum bands could be used for Wi-MAX implementation: 2.4, 2.5, 3.5, and 5.8 GHz.

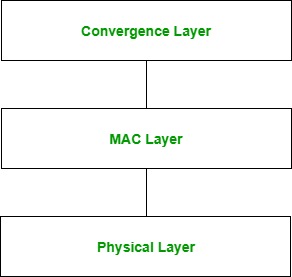
**What makes Wi-Max so special?**

• Wi-MAX is capable of fulfilling various access needs. Extension of broadband capabilities to subscribers, filling in service provider gaps in Wi-Fi, cellular backhaul, DSL, cable, and last-100-meter access from fiber to the curb are some of the potential uses. • Wi-MAX can enable very high bandwidth solutions using the current infrastructure, reducing costs while delivering the bandwidth required to support a full variety of high-value multimedia applications where significant spectrum deployments (i.e., >10 MHz) are sought.

• Wi-MAX can help service providers handle many of the challenges brought on by growing customer demands without forcing them to give up on their current infrastructure investments because it can seamlessly interoperate across several network types.

• Wi-MAX offers wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers receive the performance they expect for all forms of communications.   
• Wi-MAX, an IP-based wireless broadband technology, can be integrated with wide-area third-generation (3G) mobile, wireless, and landline networks to deliver a seamless anytime, anywhere broadband access solution.

Ultimately, Wi-MAX is intended to serve as the next stage of 3G mobile phone development—possibly by combining Wi-MAX and CDMA standards to produce 4G. Wi-MAX Goals. A standard by itself cannot achieve widespread adoption. Wi-MAX has emerged to help with adoption issues including compatibility and deployment costs. Wi-MAX will help the wireless MAN industry expand by creating and conducting compatibility testing, certifying vendor solutions with a "Wi-MAX Certified TM" label once testing is successfully completed.

**Architecture:**   
 

1. Physical Layer: This layer establishes the frequency spectrum, the multiplexing mechanism, and the synchronization of the data rates at the transmitter and receiver.   
This layer manages the encoding and decoding of signals in addition to bit transmission and reception. It converts MAC layer frames into signals that are prepared for transmission. QPSK, QAM-16, and QAM-64 are the modulation methods used in this layer.   
2. MAC Layer: This layer serves as a bridge between the convergence layer and the physical layer of the Wi Max protocol stack. It provides point-to-multipoint communication and is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The MAC layer is in charge of limiting access to shared wireless media and transmitting data in frames. The guidelines dictate when and how a subscriber can begin transmitting on the channel.

3. Convergence Layer: This layer provides access to data from outside the network. Upon acceptance, it transforms protocol data units (PDUs) at upper layers into lower layer PDUs. It provides various functions based on the service being used.

**Wi-MAX Benefits:**

1. Broad Coverage: Wi-MAX can cover an area up to 50 kilometers in diameter, making it ideal for delivering broadband connectivity in rural and underdeveloped areas.
2. High data speeds: Wi-MAX may provide data speeds of up to 75 Mbps, which is faster than many other wireless technologies.
3. Scalability: Wi-MAX can easily accommodate a large number of users and devices.
4. Interoperability: Wi-MAX is based on an international standard that allows many vendors' equipment to function with one another.
5. Economical: Wi-MAX is a cost-effective solution for providing broadband connection in locations where wired infrastructure is not commercially feasible.

**The drawbacks of Wi-MAX:**

1. Limited Mobility: Wi-MAX is designed for stationary or semi-fixed use; it is not meant for mobile use.
2. Interference: Wi-MAX and other wireless technologies may generate interference since they share the same frequency range.
3. Security Concerns: Wi-MAX may be vulnerable to security concerns like jamming and eavesdropping since it uses a shared spectrum.
4. Limited device availability: Wi-MAX devices are less widely available than those using other wireless technologies, such as Wi-Fi.
5. Limited penetration: Wi-MAX signals may not be able to fully penetrate walls and ceilings.

**Applications:**

The technology known as Wi-MAX has numerous useful applications, including:   
**Broadband Internet connectivity:** Wi-MAX is used to provide high-speed internet connectivity in underserved and rural areas where traditional wired broadband is not available.

**Wireless Backhaul:** By establishing a wireless link between a cellular base station and the core network, Wi-MAX removes the need for a cable connection.

**Mobile Broadband:** Customers can access high-speed internet while they're on the go thanks to a technology called Wi-MAX.

**Public Safety:** Wi-MAX provides wireless access to public safety networks, enabling emergency responders to communicate and exchange information in real-time.

**Wi-MAX provides** wireless communication in smart grid systems, allowing utilities to remotely monitor and control the power grid.

**Telemedicine:** Wi-MAX makes it possible for medical professionals to diagnose and treat patients remotely by providing wireless connectivity for telemedicine systems.

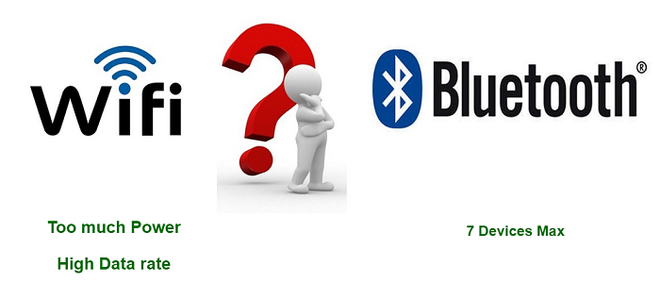
**VoIP (Voice over Internet Protocol):** Wi-MAX is also used to provide VoIP phone services using a wireless connection, allowing users to make and receive calls online.

**Video Surveillance:** Because Wi-MAX may give these devices wireless connectivity, security personnel can watch and capture video footage from a distance.

**Zig-Bee**

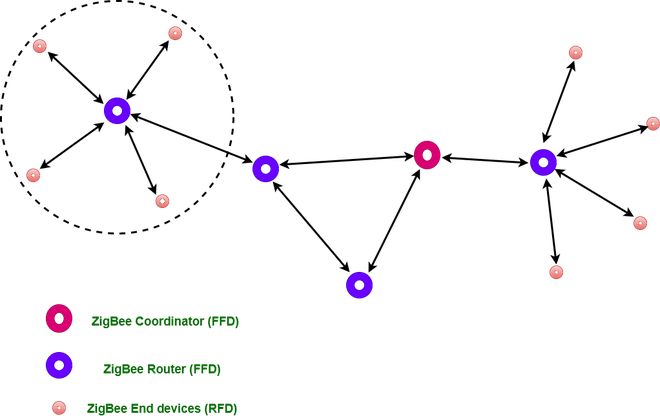
A low rate task group 4 for personal area networks is called Zig-Bee. It's a technology for home networking. Zig-Bee is a technology standard designed for network sensing and control. Based on IEEE 802.15.4, Zig-Bee was created by the Zig-bee Alliance and is the Personal Area Network of Task Group 4. The goal of the open, global, packet-based Zig-Bee protocol is to provide a low-power, secure, and stable wireless network architecture that is easy to use. Process or flow control equipment can be deployed anywhere and yet communicate with the entire system. It is also possible to relocate a sensor, pump, or valve because the network is not concerned with its precise location. IEEE802.15.4 designed the PHY and MAC layer, while Zig-Bee manages the top layers. In order to satisfy the need for low-cost, low-power, low-data-rate devices to be used for short-range wireless communications, the Zig-Bee standard was developed. IEEE 802.15.4 supports both star and peer topologies. The Zig-Bee protocol supports star and two types of peer-to-peer topologies: mesh and cluster tree. Devices using Zig-Bee technology may occasionally need to handle both point-to-point and point-to-multipoint topologies.

**Why is there need for another short-range communication protocol?**



**Zig-Bee devices come in the following types:**

• Zig-bee Coordinator Device: This device talks to routers. The devices are connected using this device.   
• Zig-bee router: This gadget facilitates data transmission between other gadgets.   
• Zig-bee End Device: This is the controlled device.



**Characteristics of the Zig-bee Protocol in General:**   
• Minimal Power Need   
• Inadequate Data Rate (20-250 kbps).   
• Confined Space (75–100 meters)   
• The approximate 30-millisecond network join time   
• Provide support for networks of any size, from 240 devices in practice to 65000 devices in theory.

• Cheap Implementation and Low Product Costs (Open Source Protocol)

• A cycle of extremely low duty.

• There are 27 channels in 3 frequency bands.

**Operating Frequency Bands (A network will only use one channel, whichever is chosen):**   
1. European Channel 0: 868 MHz

2. Channels 1 through 10: 915 MHz (Australia and the US)

3. Worldwide: 2.4 GHz Channels 11–26

**Characteristics of Zig-bee:**

1. **Stochastic addressing:** An address is announced and given to a device at random. A method for addressing and resolving conflicts. Assigned address tables do not need to be maintained by the parents node.

2. **Link Management:** Every node looks after the state of its links with nearby nodes. In routing, connection quality is equivalent to link cost.

3. **Frequency Agility:** When nodes encounter interference, they notify the channel manager, who chooses a different channel.

4. **Asymmetric Link:** The transmit power and sensitivity of each node varies. Routes could be asymmetrical. 15 seconds and 0 seconds Volume 0% This advertisement ends in 15.

5. **Power Management:** Main power is used by coordinators and routers. Batteries are used by end devices.

**Zig-bee's advantages:**

1. It uses less electricity.

2. Offers application support and network security services through IEEE standards.

3. Completely networked houses with Zig-bee enable all devices to connect and communicate with one another. Use in intelligent housing.

5. Simple to execute.

6. Sufficient security measures.

7. Low cost: Zig-bee is a cost-effective solution for Internet of Things applications since its chips and modules are reasonably priced.

9. Mesh networking: Zig-bee has a mesh network architecture, which does away with the need for a hub or router to enable device-to-device communication. This makes it ideal for use in applications related to smart homes where gadgets must communicate with one another and with a central hub in order to be controlled.

10. Reliability: The Zig-bee protocol is made to be extremely dependable, and it has strong safeguards in place to make sure that data is sent consistently even under trying circumstances.

**Negative aspects of Zig-bee:**

**1. Limited range:** When compared to other wireless communications protocols, Zig-bee's range is very low, which may make it less appropriate for use in big buildings or for some types of applications.

**2. Limited data rate:** Zig-bee might not be the greatest option for applications that require rapid data movement because it is optimized for moderate data rates.   
**3. Interoperability:** Since Zig-bee is not as widely used as other IoT protocols, it may be difficult to find devices that are compatible with one another.   
**4. Security:** Zig-bee is more vulnerable to hacking and other security issues since it has fewer strong security safeguards than other IoT protocols.

**Zig-bee network topologies include the following:**

• Zig-Bee Smart Energy's Star Topology: this configuration has a coordinator and numerous end devices; end devices only speak with the coordinator.

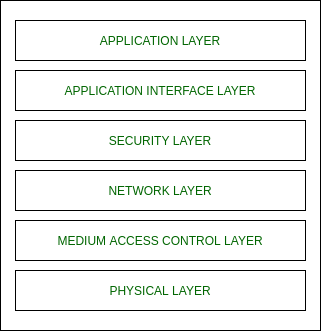
• Mesh Topology (Self Healing Process): A mesh topology consists of a coordinator, several routers, and end devices.

• Tree Topology: This topology includes of several routers, end devices, and a central coordinator node. The router's purpose is to increase the network's coverage area.

**The six levels that comprise the Zig-bee architecture are combined.**

1. Application Layer 2. Security Layer 3. Application Interface Layer 4. Network Layer

5. Medium Access Control Layer 6. The Physical Layer



**• Physical layer:** The IEEE 802.15.4 specifications cover the lowest two layers, namely the physical layer and the MAC (Medium Access Control) Layer. The Zig-bee radio is directly controlled and communicated with by the Physical layer, which is closest to the hardware. The data packets in the over-the-air bits are translated by the physical layer for transmission, and vice versa for reception.

**• MAC:** The Medium Access Control layer (MAC layer) is the layer that manages the interface between the physical and network layers. Additionally, PAN ID and network discovery through beacon requests are handled by the MAC layer.

**• Network layer:** It acts as a bridge between the MAC and application layers. It is responsible for mesh networking.   
**• Application layer:** Consisting of the application support sub-layer and the Zig-bee device object, the application layer is the highest protocol tier in the Zig-bee stack. It includes applications that the manufacturer specifies.

.

**Channel Access:**

1. Collision avoidance mechanism-equipped carrier-sense multiple access (contention-based method)   
2. Using the contention-free method, the Coordinator allots a certain time slot (a Guaranteed Time Slot, or GTS) to each device.

**Applications of Zig-bee:**

* Firstly, home automation
* Compiling Health Data
* Industrial Control Systems
* The system for reading meters
* Control system for lights
* Business
* Global Government Markets
* Networking at Home

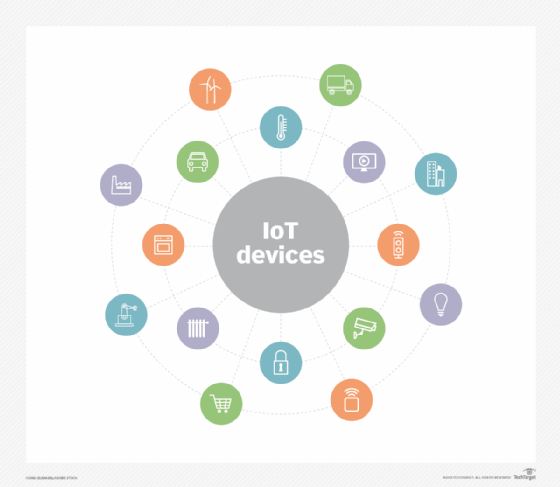
**IOT Devices**

**Internet of Things gadgets**

The internet of things (IoT) is a vast network of interconnected non-standard computing devices that may wirelessly connect to a network and transmit data. The extension of internet connectivity to a wide range of traditionally "dumb" or non-internet-enabled physical things and everyday objects, in addition to standard devices like desktops, laptops, smartphones, and tablets, is known as the Internet of Things (IoT). These technologically advanced devices have the ability to connect and communicate online. They are also remotely observable and manageable.

**What is an instance of an IoT device?**

Connected devices function together as a unit in an ecosystem, exchanging information with their surroundings and one another to automate tasks around the office and home. They are able to deliver useful sensor data to users, businesses, and other relevant parties. The devices are divided into three main groups: consumer, enterprise, and industrial. Examples of consumer-facing connected items are smart appliances, wearables, TVs, and speakers. For example, devices in a smart home are designed to detect and respond to human presence. When a person gets home, their car communicates with the garage to unlock the door. Upon entering, their smart watch data indicates that they had a stressful day; as a result, the heat and lights have already been adjusted to their favorite temperature. Other smart home equipment include sprinklers that adjust the amount of water applied to the grass based on the weather forecast and robotic vacuum cleaners that learn which areas of the house need to be cleaned most regularly. Enterprise IoT devices are edge IoT devices meant for commercial use. There are many different types of enterprise Internet of things devices available. Despite the fact that these devices have many uses, they are typically made to improve operational efficiency or maintain a facility. Among the options are smart locks, thermostats, smart lighting, and smart security systems. These technologies also exist in consumer-focused variants. In the office, smart technologies can help achieve goals. The smart sensors in conference rooms can help employees locate and reserve an appropriate meeting place while ensuring that the necessary sort, size, and amenities are accessible. When the speaker begins their presentation and the pertinent PowerPoint loads onto the screen, the lights will go out, and the temperature in the room will adjust according to the number of people present.



Some examples of consumer, business, and industrial IoT devices are smart TVs and smart sensors deployed in conference rooms and on assembly line equipment. Industrial contexts, such as factories, are the intended use for devices from the Industrial Internet of Things (IIoT). Sensors monitoring an assembly line or other industrial operation make up the bulk of IIoT devices. Applications for monitoring gather information from a range of sensors to ensure that crucial operations are running as efficiently as possible. These sensors can also aid in preventing unscheduled downtime since they can predict when parts will need to be replaced. If a problem arises, the system could be able to alert a service expert, outlining the problem and the parts that will need to be replaced. By doing this, the technician might be able to avoid going to the site to diagnose the problem and then traveling to a warehouse to get the part that's needed to fix it.

**How are IoT gadgets operated?**

Despite their differences in functionality, Internet of Things devices share many operational characteristics. First of all, objects designed for interaction with the outside world are what we refer to as Internet of Things devices. The device might be a sensor on a manufacturing line or an intelligent security camera. In either case, the device is picking up on real-world events. The device itself consists of an integrated CPU, network adapter, and firmware, which is usually developed on an open source platform. In order to receive an IP address that enables them to function on the network, Internet of Things devices frequently connect to a Dynamic Host Configuration Protocol server. Most Internet of Things (IoT) devices are designed to only work on private networks, while a tiny percentage can be accessible directly over public ones. Although it's not necessary, many Internet of Things (IoT) devices are configured and maintained by software programs. On the other hand, certain devices do not require an external program because they include built-in web servers. After an IoT device is established and operational, the vast majority of its traffic is sent forth. Security cameras, for example, stream video data. In a similar vein, an industrial sensor streams data. Smart lights are one example of an IoT device that does receive inputs.

**IoT device management: what is it?**

The successful adoption of an Internet of Things system and its connected devices may be impeded by a variety of problems, including security, interoperability, processing and power capabilities, scalability, and availability. With IoT device management, many of these issues can be fixed by using vendor services or adopting industry standards. Device management offers functions that are necessary to maintain Internet of Things (IoT) devices' security, connection, and general health over the course of their whole lives. It helps enterprises integrate, arrange, track, and remotely manage large-scale internet-enabled devices. Device configuration, provisioning, monitoring, diagnostics, troubleshooting, firmware updates, registration, activation, authentication, and authorization are among the functions that comprise these devices. Standardized device management protocols include Lightweight Machine-to-Machine and Device Management from the Open Mobile Alliance. IoT device management software and services are available from a number of vendors, including Amazon, Microsoft, Google, IBM, GE, and several more.

**Networking and connection of IoT devices**

Many aspects of the networking, communication, and connectivity protocols used with internet-enabled devices will depend on the specific IoT application being used. Much with the range of IoT applications, there are numerous networking and communication choices available. The communication protocols that are employed are AMQP, DTLS, MQTT, DDS, and CoAP. Examples of wireless protocols include IPv6, LPWAN, Zig-bee, Bluetooth Low Energy, Z-Wave, RFID, and NFC. There are further options for cellular, satellite, Ethernet, and Wi-Fi services. For any IoT application, there are intrinsic trade-offs between power consumption, range, and bandwidth that must be considered when choosing protocols and associated devices. IoT gadgets usually connect to an edge device, like an IoT gateway, from which data can be sent locally or to the cloud for analysis. Less data needs to be moved to data centers or the cloud because certain gadgets have built-in data processing capabilities. This type of processing, which typically makes use of the device's built-in machine learning capabilities, is becoming more and more popular as IoT devices generate more and more data.

**Which security threats are present in IoT devices?**

Many security and privacy-related issues arise when traditionally dumb devices are networked together. As is often the case, IoT technology has progressed more quickly than the security measures put in place to secure devices and their users. Researchers have already shown how to remotely hack automobiles and pacemakers. Large-scale distributed denial-of-service attacks known as "Mirai" disrupted services globally in October 2016, affecting DNS servers on the US east coast. The cause of the problem was identified as hackers breaking into networks through Internet of Things devices, such as wireless routers and linked cameras. Similar to this, a group of researchers demonstrated in 2015 that they could get control of a Jeep by taking use of the Controller Area Network bus and a cellular network. However, safeguarding IoT devices and the networks they connect to can be challenging due to the wide variety of IoT device types and providers as well as the difficulty of adding security to devices with constrained resources. The Mirai botnet problem was discovered to have its origins in the hacked devices' use of default passwords. Suggested IoT security techniques include network segmentation, cryptography, strong passwords, authentication/authorization, and identity management. Fearing risks from the constantly growing attack surface of the Internet of Things, the FBI released a public service announcement in September 2015 under FBI Alert Number I-091015-PSA. It outlines the risks connected to IoT devices and provides preventative measures and solutions for mitigation. The U.S. Senate introduced the IoT Cyber security Improvement Act in August 2017, a bill that addresses security flaws associated with IoT devices. In an effort to further improve cyber security related to IoT, a further act called as the Internet of Things Cyber security Improvement Act of 2020 required that NIST develop and distribute guidelines and standards for the management and use of IoT devices. These standards are meant to be used by federal agencies, but the private sector will most likely also adopt them.

**IoT device trends and projected expansion**

Forecasts on the proliferation of IoT devices in the future have been rapid. On the upper end of the spectrum, Intel predicted that by 2020, there will be 200 billion internet-enabled gadgets worldwide, or almost 26 smart devices for every person on the planet, up from 2 billion in 2006. A little more pessimistic, IHS Market estimated that by 2025 there will be 75.4 billion connected devices, and by 2030 there will be 125 billion. Some companies have cut staff by not including PCs, iPads, or cell phones. Gartner projects that there will be 20.8 billion connected devices in use by 2020; IDC projects 28.1 billion, while BI Intelligence projects 24 billion. Using IoT devices effectively means understanding how the edge and IoT are intertwined, and making sure your IoT strategy gets off to a solid start. Whether your firm is considering integrating IoT devices or is already using them, be sure you're prepared to handle the unique security challenges they present.