Cisco NETACAD Connecting Things Chapter 4

Chapter 4: Networks, Fog and Cloud Computing

Personal information related to health, location, wealth, personal preferences and behaviors is passing through the IoT devices in increasing volumes. This increase in volume elevates the relevance of increasing the attention on data privacy and data protection.

New wireless technologies and protocols, such as ZigBee, Bluetooth, 4G/4G, and LoRaWAN, have been developed to accommodate the diversity of IoT devices. Wireless technology is selected based on the range of coverage, bandwidth requirements, power consumption, and deployment location.

Wireless security considerations include: selecting a secure protocol, protection for management frames, identification of frequency jamming, detecting rogue access points, and using security at the application layer.

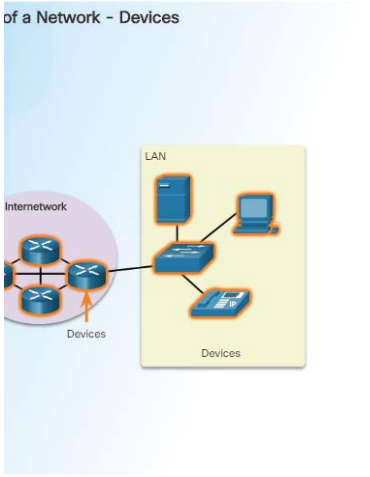
Cloud computing is a service that offers off-premise, on-demand access to a shared pool of configurable computing resources. Cloud computing offers services such as IaaS, PaaS, mPaaS and SaaS.

A fog computing model identifies a distributed computing infrastructure closer to the network edge. It enables edge devices to run applications locally and make immediate decisions.

The proliferation of devices in the IoT is one of the primary reasons for the exponential growth in data generation. Data can be deemed at rest or in motion. Big Data is typically characterized in three dimensions: volume, velocity, and variety.

Data stored in servers must be encrypted to avoid data tampering or theft. Regular backups are mandatory to minimize losses in case of a disaster.

IoT devices should run the latest version of firmware and protocols and any communication between devices should be done using protocols that provide secure encryption by default.



LAN and WAN

The purpose of networks is to allow the transmission of messages among various connected devices. Historically, the main characterization of networks was based on the geographic scope and the span of the administration of the network. Networks were categorized as local-area networks (LANs) or wide-area networks (WANs). The added diversity and number of connected devices and the different connectivity needs of the IoT devices has given rise to newer variations of network types. Connecting servers in a data center is a different problem than connecting wireless microcontrollers in a car or connecting parking lot sensors to controllers. Even though the connection requirements are different, the fundamental networking systems that support each of these different needs are basically the same.

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another, or as complex as a collection of networks that literall spans the globe. The network infrastructure has three categories of network components:

- Devices
- Media
- Services

Figures 1 through 3 represent the network components.

routers, switches, and wireless routers.

Communication across a network is carried on a medium. The medium provides the physical channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted, as shown in Figure 4.

- **Metallic wires within cables** - data is encoded into electrical impulses
- **Glass or plastic fibers (fiber-optic cable)** - data is encoded as pulses of light
- **Wireless transmission** - data is encoded using radio waves

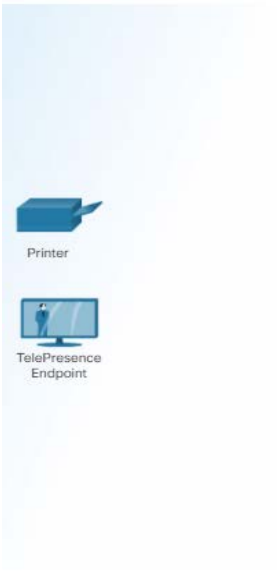
Different types of network media have different features and benefits. Not all network media have the same characteristics, nor are they all appropriate for every purpose. For example, wireless technologies that connect sensors can have different characteristics in the following areas:

- the range of use from a few centimeters to many kilometers
- the amount of bandwidth from a few kilobits per second up to gigabits per seconds
- the amount of power consumption from nanowatts to a few watts

Choosing the appropriate technology is an important design decision that depends on the specific IoT application.

Figure 5 displays criteria to consider when choosing network media.

Network Devices and Communication Media



Network devices are devices that connect to each other through a network. The traditional network devices that people are most familiar with are called end devices. Some examples of end devices are shown in Figure 1. In the IoT space, everything can become a networked device. Figure 2 shows examples of household end devices. To see a collection of consumer electronics connected devices click here.

An end device is either the source or destination of a message transmitted over the network, as shown in the animation in Figure 3. To distinguish one end device from another, each end device on a network is identified by an address. When an end device initiates communication, it uses the address of the destination end device to specify where the message should be sent.

Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. These intermediary devices provide connectivity and ensure that data flows across the network.

Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network. Examples of the more common intermediary devices are gateways, routers, switches, and wireless routers.

Communication across a network is carried on a medium. The medium provides the physical channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect

---

of a newer use of the LAN definition that has grown to support the IoT. In this case, it is common to hear the expression "Factory Floor" to indicate the specific area occupied by the industrial machines. The term "Industrial Internet" often specifies the devices that can operate in the industrial environment. This environment is characterized by a high level of dust, noise, temperature variations, and mechanical vibration. Ethernet based technologies are still used in these situations but more and more wireless technologies are emerging as the best approach to supporting smart factories and other "non-typical" environments.

A WAN is a network infrastructure that spans a wide geographical area. WANs are typically owned by enterprises or by Internet Service Providers. WANs are often managed by service providers (SP) or Internet Service Providers (ISP). An enterprise network may be managed internally but use WAN services from an ISP.

Specific features of WANs include the following:

- WANs interconnect LANs over wide geographical areas such as cities, states, provinces, countries, or continents.
- WANs can include network segments administered by multiple service providers.
- WANs typically provide slower speed links between LANs.

The traditional internet WAN uses mostly wired technologies and the system is connected to the electric grid for the power. Often in the case of IoT WANs, the interconnection could use wireless links and battery powered sensors. Because of these new constraints, a new class of WAN technologies has emerged named Low Power Wide Area Networks (LPWAN) that allow low bandwidth wireless interconnections of battery powered devices spread in a geographical area.

Devices and media are the physical elements, or hardware, of the network. Hardware usually consists of the visible components of the network platform such as laptops, PCs, switches, routers, wireless access points, or the cabling that is used to connect the devices.

Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

A LAN is a network infrastructure that spans a small geographical area. Specific features of LANs include:

- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
- A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies are enforced at the network level.
- LANs provide high speed bandwidth to internal end devices and intermediary devices.

A Personal Area Network (PAN) is a type of LAN useful to the IoT. A PAN is a network that spans a few meters around the individual, usually using wireless technology. A PAN is meant to interconnect devices like wearables, mobile phones, headsets and any other personal technology. Often it uses short rage wireless technologies like Bluetooth.

A LAN used to connect machines in the factory plant is one example of a newer use of the LAN definition that has grown to support the IoT. In this case, it is common to hear the expression "Factory Floor" to indicate the specific area occupied by the industrial machines. The term "Industrial Internet" often specifies the devices that can operate

Network Protocols

While proper media is required for device communication, it is not enough. Devices must conform to common communication rules before they can communicate. These rules are called protocols.

Similar to human languages, network devices take advantage of specific communication rules to ensure the messages are sent and received, and that they can be understood. Two very important families of protocols are Ethernet and TCP/IP.

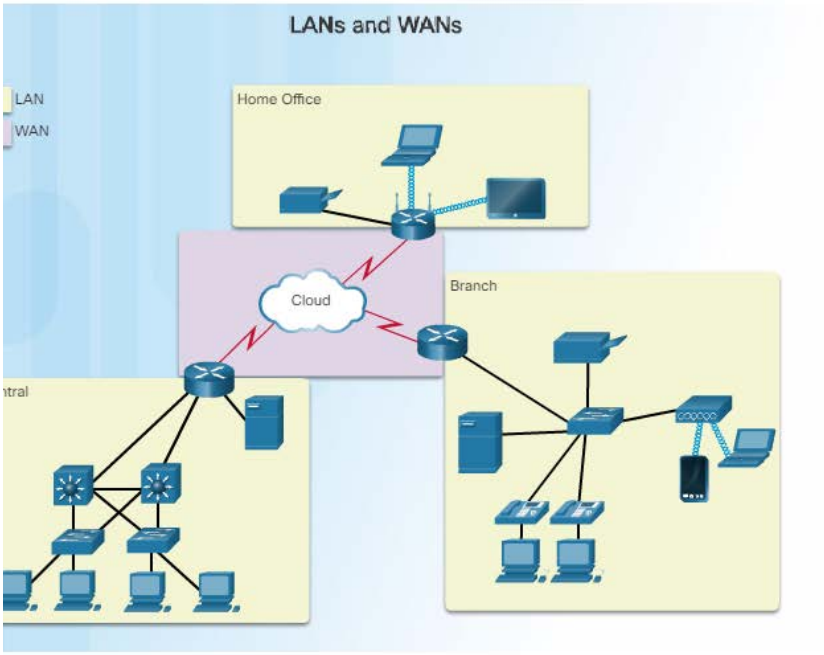
Ethernet is a family of technologies and protocols ruling the communication between local devices, ensuring they can successfully communicate while sharing the same communication media. Without Ethernet, signals placed on shared network media by network devices could interfere and become unreadable.

TCP/IP is the family of protocols that interconnects billions of devices from networks throughout the Internet. Notice that while Ethernet and TCP/IP are both communication protocols, they have very distinct functions and roles in network device communication. Ethernet ensures proper use of the local media, while TCP/IP facilitates remote communication and is independent of the media. A network device is said to support a specific network protocol when the network device has been configured or programmed to send and receive messages that conform to the rules defined by the supported network protocol.

In the IoT domain, new protocols are emerging that enrich the TCP/IP suite and deal with the specific requirements of the IoT. Many common emerging IoT applications such as industrial automation, smart agriculture, and smart cities, require networks that support large scale wireless data acquisition and feedback loops on actuators that are based on low-powered embedded devices.

These networks often have connections that are typically less reliable than the typical office IT networks. Some of these new networks called Low Power and Lossy Networks (LLN) tend to have lower transmission speeds and a higher packet loss rate due to several factors such as small antennas, CPU, memory, power and environmental factors. While Ethernet and TCP/IP are still universally recognized as the key protocols for the Internet, the protocols that are required to support the IoT are still evolving.

Note: The specific rules and mechanisms implemented by emerging protocols are beyond the scope of this course. Click here for more information.



Basic Routing

The Internet is comprised of LANs interconnected by WAN links. In order to move from one LAN to another (source to destination), packets must cross one or more networks. In that scenario, LANs and WANs act as the transit paths for packets.

The process of directing a packet towards its destination is called routing and is the main function of a router. Routers are intermediary network devices. They are responsible for directing packets through networks, towards their final destination. Be it local routing (routing packets within LANs) or remote routing (routing packets between LANs) routers are crucial intermediary network devices. Because there may be multiple routes for a packet to take from source to destination, it is also a responsibility of a router to choose the best route.

The figure shows LANs and their respective WAN links.

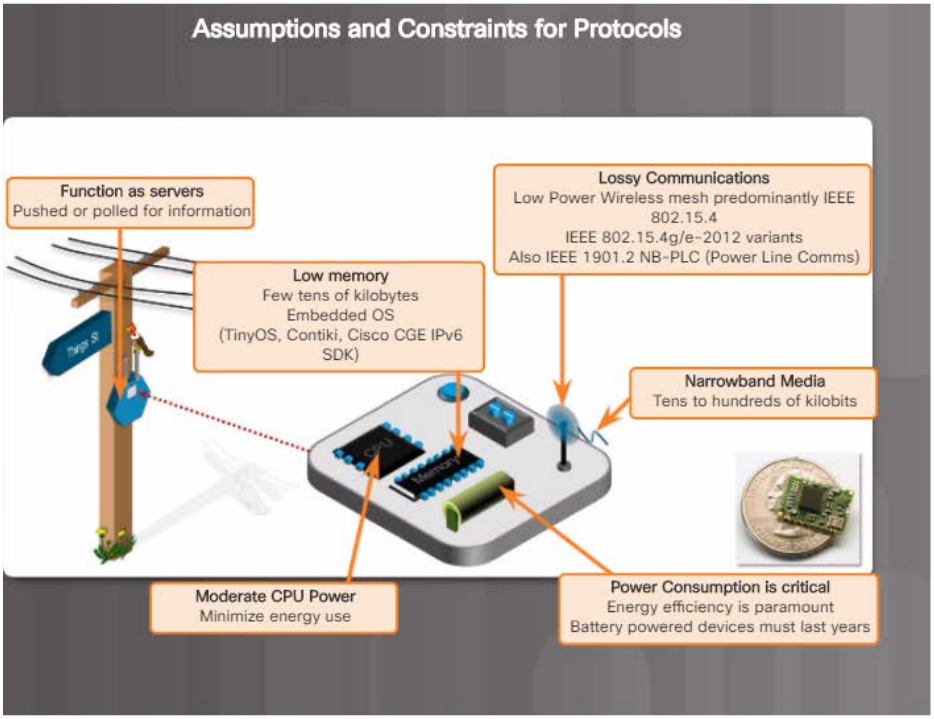
End devices that operate on Low Power or Lossy Networks (LLN) are constrained by power, memory, low data rates, and environmental issues. Routers used in the same "non-traditional" environments also have the same constraints. New routing protocols are emerging to support routers in these unstable situations.

Note: The details of how routers choose the best path from source to destinations are out of the scope of this course.

All devices connected to the Internet must have a unique identifier. The Internet Protocol (IP) defines and implements this unique identifier as an **IP address**. Because IP is the most popular communication protocol used on the Internet today, if a device wants to connect and communicate on the Internet, it must conform to the rules of IP.

All local devices must be configured with unique IP addresses. Local devices must also be configured with the IP address of the default gateway they have to use to reach remote networks. When the configuration is complete, local devices can communicate among themselves directly, by using their unique IP addresses. If a local device wants to communicate with a remote network, it must send the packet to the default gateway, as the default gateway is the exit point for the LAN.

A local device configured with a unique IP address but not configured with the address of its default gateway, can still communicate locally but will not be able to communicate with any remote networks.

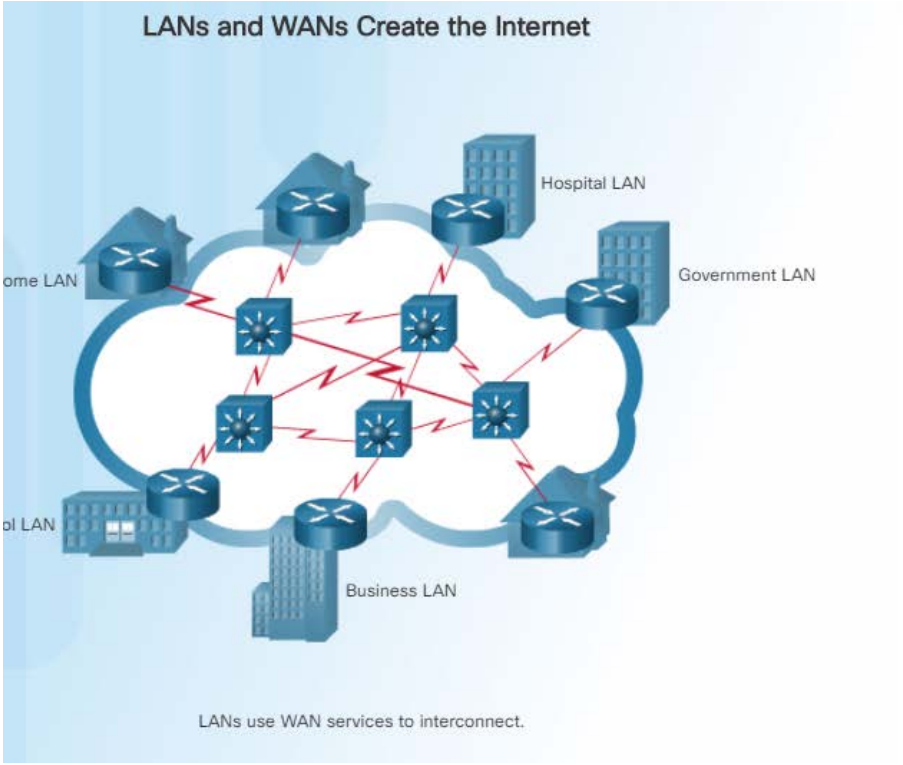


IoT Protocols

IoT devices tend to be embedded devices with small amounts of memory and limited power availability. Because IoT devices are often deployed under suboptimal conditions such as outdoors, on manufacturing floors or inside the human body, some basic requirements such as power and network connectivity are likely to be constrained. These challenges force IoT designers to work with a different set of protocols created specifically for the IoT and its particular challenges.

While most of the success of the Web is based on the use of a Client/Server approach using the HTTP protocol for exchanging messages, in the case of the IoT networks different approaches are emerging. CoAP and MQTT are two data protocols common in the IoT.

CoAP (Constrained Application Protocol) is a protocol intended for resource-constrained IoT devices that enables IoT devices to communicate with the Internet. CoAP is based on HTTP and the REST model where resources are retrieved from a server using URIs/URLs, The clients use the well-

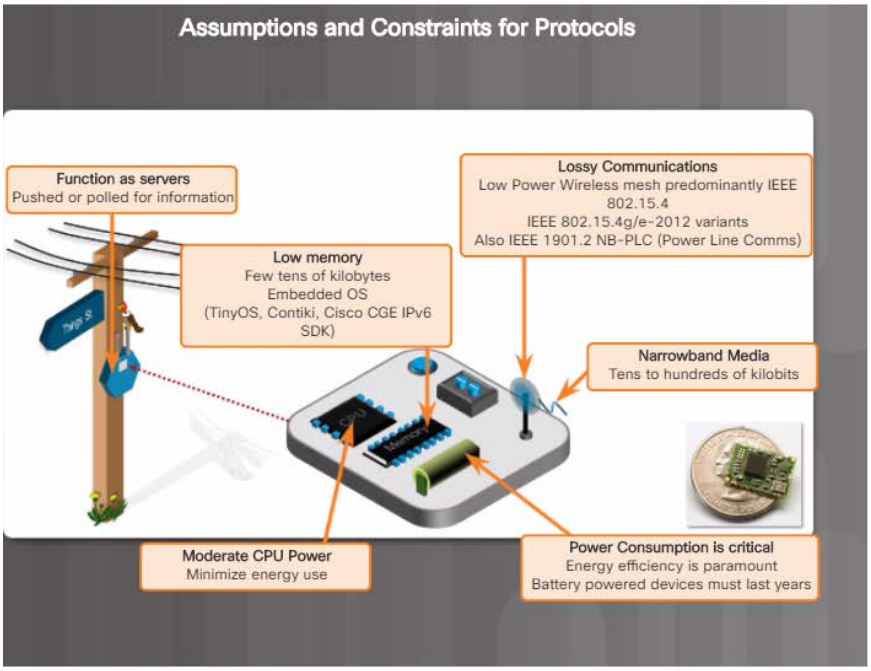


LANs use WAN services to interconnect.

LANs, WANs and the Internet

In a small office or home office (SOHO), it is common to employ a single router. This router is responsible for providing connectivity to all local devices (computers, tablets, smartphones and smart appliances), through a wired or wireless connection. The SOHO router also acts as a connection point between the SOHO network and the Internet. In this scenario, the SOHO network is a LAN, connected to all other LANs (the Internet) via a WAN link. The WAN link comes from a local Internet service provider (ISP). This ISP WAN link connects to the SOHO router via a special port, designed specifically for a WAN connection.

For the SOHO local devices, the SOHO router is the only way to reach remote networks. Because of this, the SOHO router acts as the **default gateway** for all the SOHO local devices. When packets are to be sent to remote destinations, all SOHO local devices know they must send the packet to the default gateway.



IoT Protocols

IoT devices tend to be embedded devices with small amounts of memory and limited power availability. Because IoT devices are often deployed under suboptimal conditions such as outdoors, on manufacturing floors or inside the human body, some basic requirements such as power and network connectivity are likely to be constrained. These challenges force IoT designers to work with a different set of protocols created specifically for the IoT and its particular challenges.

While most of the success of the Web is based on the use of a Client/Server approach using the HTTP protocol for exchanging messages, in the case of the IoT networks different approaches are emerging. CoAP and MQTT are two data protocols common in the IoT.

CoAP (Constrained Application Protocol) is a protocol intended for resource-constrained IoT devices that enables IoT devices to communicate with the Internet. CoAP is based on HTTP and the REST model where resources are retrieved from a server using URIs/URLs, The clients use the well-known methods of GET, PUT, POST, and DELETE to manipulate these resources. CoAP can be used via other mechanisms, such as SMS on mobile communication networks.

CoAP is designed to provide multicast support, low overhead, and simplicity. It is designed to work on microcontrollers with as low as 10 KB of RAM and 100 KB of storage space while also providing strong security.

A different approach is provided by the MQTT protocol. MQTT (Message Queuing Telemetry Transport) is a lightweight protocol. MQTT is best suited for systems that rely on low bandwidth connections and require code with a small footprint. MQTT protocols uses the concept of publish-subscribe communications among nodes.

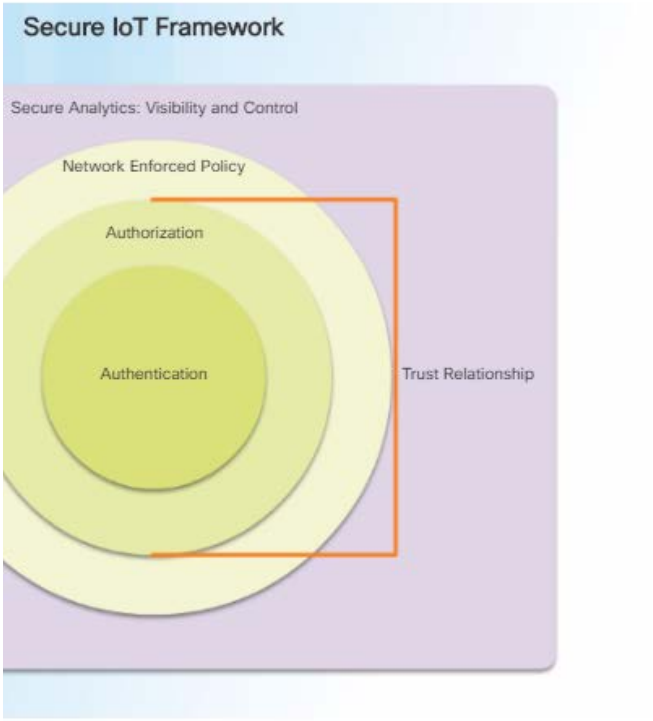
The publish-subscribe schema requires the presence of an intermediate node called a message broker. Every source of data must publish the data element on the broker node indicating to which "topic" the data belongs. The nodes interested in receiving data on a specific topic must subscribe to that topic on the broker. The broker will then distribute the messages to interested clients based on the topic of a message.

More information about MQTT can be found at http://mqtt.org/

should use strong encryption and authentication schemes where possible. New authentication and authorization protocols are in the process of development. As an example, the National Institute of Standards and Technology (NIST) are currently working on a new compact version of the secure hash algorithm SHA-3 to be used for embedded or smart devices.

The figure shows an example of a Secure IoT Framework. It outlines the following components:

- Authentication – IoT devices connecting to the network create a trust relationship based on valid identity through mechanisms such as: passwords, tokens, biometrics, RFID, X.509 digital certificate, shared secret, or endpoint MAC address
- Authorization – a trust relationship is established based on authentication and authorization of a device that determines what information can be accessed and shared
- Network Enforced Policy – controls all elements that route and transport endpoint traffic securely over the network through established security protocols
- Secure Analytics: Visibility and Control – provides reconnaissance, threat detection, and threat mitigation for all elements that aggregate and correlate information



Securing the IoT Network

IoT devices are becoming more common in our daily lives. As the IoT gets more integrated into the daily activities of people, IoT devices handle more sensitive data. Personal information related to health, location, wealth, personal preferences and behaviors is passing through the IoT devices in increasing volumes. This increase in volume elevates the relevance of increasing the attention on data privacy and data protection.

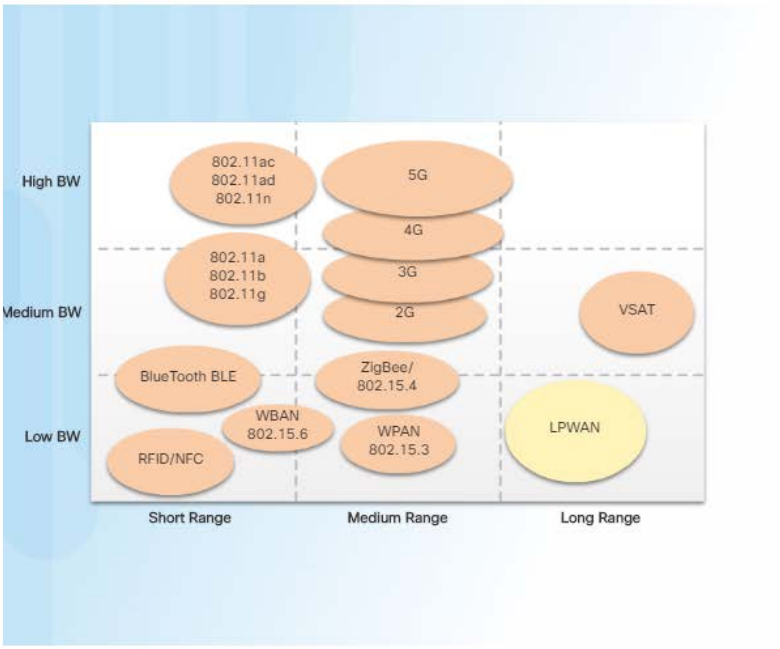
To address data privacy, system designers need to ask questions such as the following: What data can be collected? What form of consent is required? Who should be allowed to see the data?

Many IoT applications generate traceable signatures of the location and behavior of the users. This process works against data privacy. To combat this, IoT devices need to be able to verify device ownership and the identity of the owner while decoupling the device from the owner. This is a process called shadowing. A digital shadow enables user objects to act on a user's behalf using a virtual identity.

Data security needs to ensure that the data does not leak outside of the designed application or that the data is not altered or deleted by means of a security attack. A fundamental element in securing the network is device identity and mechanisms to authenticate them. Devices should use strong encryption and authentication schemes where possible. New authentication and authorization protocols are in the process of development. As an example, the National Institute of Standards and Technology (NIST) are currently working on a new compact version of the secure hash algorithm SHA-3 to be used for embedded or smart devices.

The figure shows an example of a Secure IoT Framework. It outlines the following components:

- Authentication – IoT devices connecting to the network create a trust relationship based on valid identity through mechanisms such as: passwords, tokens, biometrics, RFID, X.509 digital certificate, shared secret, or endpoint MAC address
- Authorization – a trust relationship is established based on authentication and authorization of a device that determines what information can be accessed and shared
- Network Enforced Policy – controls all elements that route and transport endpoint traffic securely over the network through established security protocols
- Secure Analytics: Visibility and Control – provides reconnaissance, threat detection, and threat mitigation for all elements that aggregate and correlate information



WiFi

One of the biggest areas of growth for the IoT are wireless devices. Many new wireless technologies and protocols have been developed to accommodate the diversity of these new devices and their different requirements for connectivity. ZigBee, Bluetooth, 4G/4G, and LoRaWAN are some examples of these wireless technologies.

Some of the wireless protocols are designed for short range networks, some for medium, and some for long range. Figure 1 shows a graph categorizing the different protocols by the range that they support.

Low-Power Wide-Area Networks (LPWAN) is a wireless communications network designed to support long range communications for low bit rate devices such as sensors, actuators, and controllers. LPWANs provide excellent coverage in urban, rural, and remote areas. The signal area extends from 5 to 40 kms depending on the openness of the geography. The base stations have a battery life of 10 years and they support thousands of devices. Examples of LPWAN protocols are LoRaWAN, Weightless-N, and RPMA.

System designers will select the wireless technology based on the range of coverage, bandwidth requirements, power consumption, and deployment location. Figure 2 compares wireless topologies based on these criteria.

Bluetooth

Bluetooth is a wireless protocol used for data communication over short distances. Bluetooth is now supported by almost all mobile devices and accessories and is the defacto standard for audio between mobile devices. Communication between Bluetooth devices takes place through a short range wireless network called a personal area network (PAN).

Originally described under IEEE 802.15.1, Bluetooth is now maintained by The Bluetooth Special Interest Group (SIG) which oversees development of the specification, manages the qualification program, and protects the trademarks. Manufactures who want to market products as Bluetooth devices must meet Bluetooth SIG standards.

Bluetooth operates at the industrial, scientific and medical (ISM) 2.4 GHz short-range radio frequency band. Bluetooth was invented by Ericsson in 1994 and is defined as a packet-based protocol. It works based on a master-slave structure. The Bluetooth specification is mature and has gone through several version iterations.

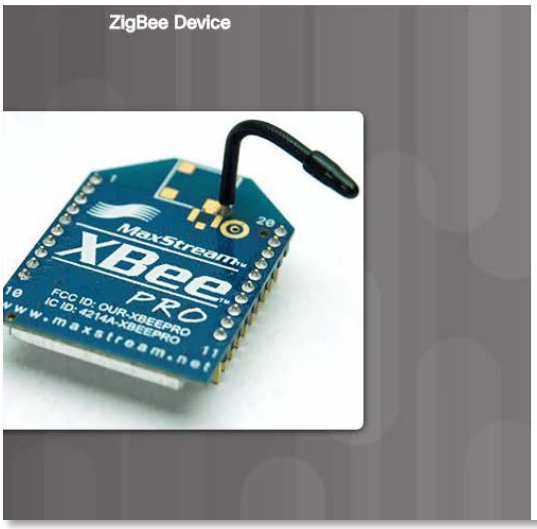
Very relevant for the IoT is Bluetooth Low Energy (BLE) also known as Bluetooth Smart. BLE has become very popular because of the support of the smartphone industry and because of new applications in healthcare, fitness, and beacons. Bluetooth Low Energy operates in the 2.4 GHz ISM band. It has a very fast connection rate (milliseconds) and a very high data rate (1 Mbps). The BLE device then goes into

band. It has a very fast connection rate (milliseconds) and a very high data rate (1 Mbps). The BLE device then goes into "sleep mode" until a connection is reestablished. Doing so ca lengthen the battery life for several years.

Beacons use BLE technology and the BLE technology is built into most smart phones. Beacons are small nodes (smaller than a computer mouse) that can be placed almost anywhere They may be positioned on buildings, in coffee shops, and on light posts. Their main purpose is to provide location services As an example, if a person with a smartphone, that is BLE-enabled, walks near a beacon, the beacon will send the beacon location to the smartphone. It is then up to the smartphone application to determine what to do with the location information. This is a form of one-way communication. One-way beacons do not require a paired connection.

The growth of BLE-enabled phones is growing rapidly. Because of this, the smartphone industry is interested in expanding the use of beacons as a way of doing Location Based Services.

Bluetooth 5 was announced by the Bluetooth SIG in June 2016. Version 5 has four times the range and is twice as fast as earlier versions. When operating in low energy mode, Bluetooth 5 achieves an eight-fold increase in data broadcasting capacity over Bluetooth 4.x. This is very important for IoT devices which rely on constricted power sources. Bluetooth 5 bandwidth is defined at 2 Mbps but allows for bandwidth that can be adjusted depending on the application.



ZigBee is a low-energy, low-power, low-data rate wireless protocol specification used to create personal area networks. Areas of utilization include home automation, medical device data collection, and other low-power low-bandwidth needs. Built on top of the IEEE 802.15.4-based standard specification, ZigBee is designed to be simpler and cheaper than other wireless personal area networks, such as Bluetooth or Wi-Fi. ZigBee-based applications include wireless light switches, electrical meters with in-home-displays, traffic management systems, and other consumer and industrial equipment that requires short-range, low-rate wireless data transfer.

ZigBee low power, low-cost wireless networks are commonly used with long battery life devices that are used in wireless control and monitoring applications. The ZigBee specification defines a 250 kbps transfer rate and is best suited for intermittent data transmissions.

Operating in the industrial, scientific and medical (ISM) radio bands, ZigBee has become very popular for use on IoT devices. To include ZigBee capabilities in their devices, IoT designers tend to use ZigBee chips, integrated with radios and with microcontrollers.

The ZigBee specification relies on a main device called a ZigBee Coordinator. Tasked with managing all ZigBee client devices, the ZigBee Coordinator, is responsible for the creation and maintenance of the ZigBee network. The coordinator can talk to up to eight endpoints or routers in any combination. If an endpoint is too far away from the controller, a ZigBee router can be used to bridge data between the coordinator and the endpoint.

Figure 1 shows a ZigBee device. Figure 2 shows a few ZigBee topologies and device roles

Every data request sent to or received from ZigBee uses an Application Profile Identification Number. Application profile ID numbers are 16-bit numbers that relate to public profiles, manufacturing profiles, or private profiles.

As an example, home automation is a public application profile. This profile defines ZigBee networked devices intended for use in the home, such as wall switches, thermostats, heaters, air conditioners, and keyless entry systems. This profile ensures that devices from one manufacturer will interact with devices from another.

Private profiles are used for applications where different vendor devices do not need to interact.

Figure 3 shows a chart with some of the ZigBee public profile IDs.

4G/5G

Cellular-based data networks are also an option for the IoT. This mature technology makes it possible for IoT devices to take advantage of communications over large geographic areas.

In the last 30 years the mobile industry has evolved exponentially; starting from the First Generation (1G) in the 1980s, the Second Generation (2G) in the 1990s, the Third Generation (3G) in the 2000s, the Fourth Generation (4G) in the 2010s, and now the emerging Fifth Generation (5G) expected for 2020.

Fourth Generation (4G) is the current cellular-based technology for transferring data. The International Mobile Telecommunications Advanced (IMT-Advanced) standard defines the bandwidth of any 4G system as 100 Mbps for high mobility communication such as from trains and cars and 1 Gbps for low mobility communication such as pedestrians and stationary users. The high bandwidth supported by 4G systems allows for a number of applications to be supported on mobile platforms. It provides support for voice, IP telephony, mobile Internet access, video calling, gaming services, cloud computing, high-definition mobile TV, and mobile 3D TV. Long Term Evolution (LTE) and WiMAX (IEEE 802.16e) are two popular 4G systems.

devices, the technology is still expensive. Cellular carriers insist on monthly payments tied to data caps. In addition to that, the hardware required to access a cellular network is also expensive, primarily due to intellectual property and the use of licenced radio frequency spectrums.

The term 5G, short for 5th generation, is the proposed next telecommunications set of standards to replace the current 4G/IMT-Advanced standards. 5G research and development improve IoT communications, by lowering cost, lowering battery consumption, and lowering latency.

The Next Generation Mobile Networks Alliance defines the following requirements that a 5G standard should fulfill:

- Data rates of tens of megabits per second for tens of thousands of users
- Data rates of 100 megabits per second for metropolitan areas
- 1 Gb per second simultaneously to many workers on the same office floor
- Several hundreds of thousands of simultaneous connections for massive wireless sensor networks
- Spectral efficiency significantly enhanced compared to 4G
- Improved coverage
- Enhanced signaling efficiency

The latest release of LTE 4G technology is release 13e which includes the standardization of NarrowBand IoT (Or NB-IoT) that is a LPWAN technology.

Although cellular data networks are a great way to connect IoT devices, the technology is still expensive. Cellular carriers insist on monthly payments tied to data caps. In addition to that, the hardware required to access a cellular network is also expensive, primarily due to intellectual property and the use of licenced radio frequency spectrums.

LoRaWAN

LoRaWAN is a network protocol intended for wireless battery-operated things in regional, national or global networks.

LoRaWAN is wireless technology designed to provide wireless WAN connections to power constricted devices. Categorized as a Low Power Wide Area Network (LPWAN), LoRaWAN targets key requirements of the Internet of Things such as secure bi-directional communication, mobility and localization services.

LoRaWAN architecture is often laid out in an extended star topology (star-of-stars) in which gateways relay messages between end-devices and a central network server is located in the backend. Acting as transparent bridges, gateways connect to LoRaWAN network servers via standard IP connections. LoRaWAN end-devices use wireless communications to the gateway to achieve full Internet connectivity.

LoRaWAN data rates range from 0.3 kbps to 50 kbps. LoRaWAN network servers manage the rate of data exchange with each device, using a technology called Adaptive Data Rate (ADR), to maximize both the battery life of the end-devices and the overall network capacity. Security is built into the LoRaWAN standard, implemented in a multi-layer encryption scheme. Unique keys are used in the Application, Network, and Device layers.

Securing the Wireless

Cisco NETACAD Connecting Things Chapter 4

Network

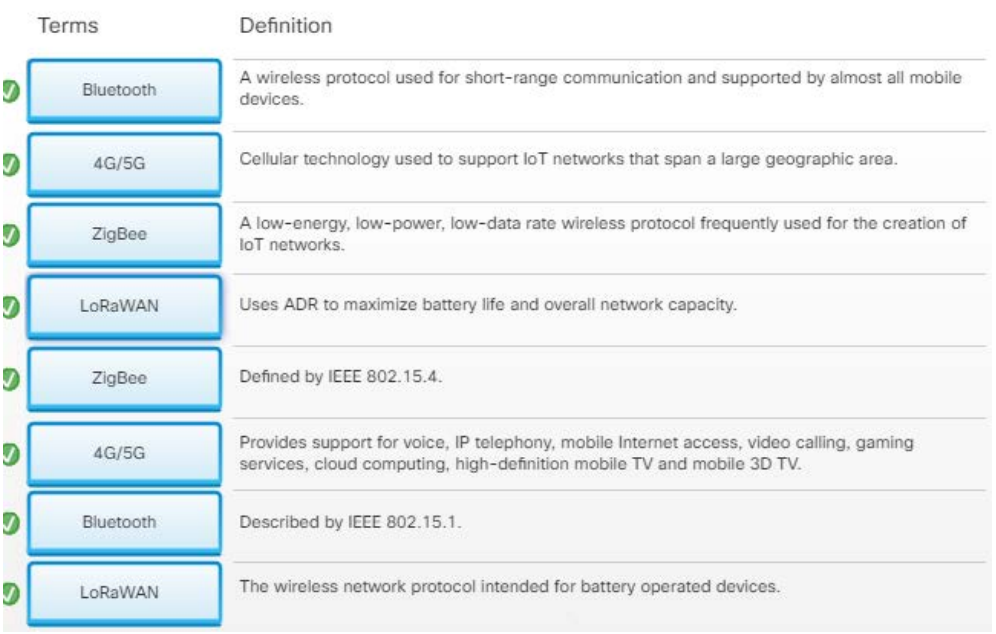
Because of their nature, wireless networks have no clear boundaries. Securing wireless communications requires strong encryption, authentication, and secure protocols.

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. Wireless networks using WEP or WPA/TKIP are not very secure and are vulnerable to hacking attacks.

WPA2 implements AES, a strong encryption algorithm, and is more secure than WPA. WPA2, an interoperable implementation of 802.11i, is currently the most commonly deployed option in wireless security. Wireless networks using WPA2/AES should have a pass phrase of at least 21 characters. If an IPsec VPN is available, it should be used on any public wireless LANs. WPA2 also has an additional feature called protected management frames. This feature protects unicast and multicast management frames from eavesdropping and forging.

Authentication is now a fundamental component of enterprise wireless policy. The 802.11i architecture specifies 802.1X for authentication, entailing the use of EAP and an authentication server.

Click here to watch a video highlighting the vulnerability of using an insecure wireless hotspot in a coffee shop.



Terms	Definition
Bluetooth	A wireless protocol used for short-range communication and supported by almost all mobile devices.
4G/5G	Cellular technology used to support IoT networks that span a large geographic area.
ZigBee	A low-energy, low-power, low-data rate wireless protocol frequently used for the creation of IoT networks.
LoRaWAN	Uses ADR to maximize battery life and overall network capacity.
ZigBee	Defined by IEEE 802.15.4.
4G/5G	Provides support for voice, IP telephony, mobile Internet access, video calling, gaming services, cloud computing, high-definition mobile TV and mobile 3D TV.
Bluetooth	Described by IEEE 802.15.1.
LoRaWAN	The wireless network protocol intended for battery operated devices.

When a WiFi-based IoT device or wireless network is being designed, several security considerations should also be kept in mind such as: selecting a secure protocol, protection for management frames, identification of frequency jamming, detecting rogue access points, and using security at the application layer.

One of the most common wireless security threats is the presence of rogue access points. A rogue access point is not approved by administration but is working on the secure network anyway. These rogues can be setup by employees looking for free wireless access or by intruders with more devious intentions in mind. Security administrators should publish and enforce strict rules concerning rogue APs, employ active access point scanning to detect rogues, and use authentication between devices on the network.

Select a wireless protocol with robust, proven security. Many protocols such as LoRoWAN and Bluetooth provide excellent encryption. Although ZigBee is one of the global standards of communication and is very easy to implement, it is not perfect yet. At the time of writing, ZigBee version 1.2 has a number of serious and exploitable security vulnerabilities. Most of these protocol design flaws relate to attempts to make it easier for the end-user to add a ZigBee device to the ZigBee network. Because of these vulnerabilities, ZigBee version 1.2 should not be used on mission critical applications.

Even though most protocols have comprehensive security methods, it is still possible for attacks to be launched against cellular networks. Because user data confidentiality is a cellular carrier responsibility, these attacks would increase the risk of a data breach when data is being transmitted over cellular networks. For this reason it is recommended that security in the form of data authentication and encryption is implemented as part of the application using technologies such as VPNs and TLS/SSL.

With its "pay-as-you-go" model, cloud computing allows organizations to treat computing and storage expenses more as a utility rather than infrastructure. In business terms, this means that initial costs required to setup an IT infrastructure (capital expenditure) are now transformed into operating expenditures.

Currently, there are over 3,000 data centers in the world that offer general hosting services to organizations. There are many more data centers that are owned and operated by private industries for their own use.

Cloud computing offers services in the following areas:

- Infrastructure as a Service (IaaS) – Hardware including servers and other infrastructure components are supplied by a provider and adjusted on-demand. The provider handles system maintenance, backups and continuity planning.
- Platform as a Service (PaaS) – A provider provides the platform, servers, storage, and OSs for users to develop and launch applications.
- Mobile PaaS (mPaaS) – Providers supply development capabilities for mobile application designers and developers.
- Software as a Service (SaaS) – Software, such as messaging, IoT data processing, payroll processing, gaming, and tax preparation is licensed on a subscription basis and hosted on cloud servers.

Cloud Services

Cloud services are services offered by cloud providers that are hosted off-premise and available on-demand. Cloud customers have access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort.

Because of the high availability and great resource scaling properties of cloud services, these services are a great way to extend the functionality of an IoT system. Data processing and storage can be done in the cloud instead of in the IoT devices. Because the services are all hosted in the cloud, data and resources are always available to any device in the system as long as the device has Internet connectivity. Cloud service providers are also very serious about security, ensuring customer data is kept safe and secure.

IoT systems that require server communications such as cloud data analysis could benefit greatly from a cloud computing service. The following are examples of cloud services:

Amazon AWS: Cloud computing is a cloud service that provides cloud-hosted, on-demand computing as a service. With cloud computing, a user can deploy and start using computers in a matter of minutes. Because the service is designed to be on-demand, users can start with low hardware resources (memory and CPU) and expand as needed. Amazon provides a great cloud computing service called AWS.

IFTTT: Short for 'If This Then That,' IFTTT allows for special resource URLs to be created and mapped to specific IFTTT actions. Imagine you want to receive an SMS message on your cellphone every time someone walks in front of your house. You can easily install a motion sensor-capable IoT device to track movement but the exchange between that device and the cellular messaging system will take some work. IFTTT masks that complexity by allowing your movement tracking device to send SMS messages by simply accessing a web URL every time the motion sensor detects movement. Many actions are currently supported by IFTTT, making it a useful cloud service for IoT.

Zapier: Similar to IFTTT, Zapier also allows for cloud-based automation. The main difference between the two services is that Zapier is more business-driven, supporting more applications and actions. Another important difference is that Zapier is only free if you have up to five actions (or zaps, as called by Zapier) configured. If more zaps are needed, a paid account must be created.

Built.io: This is a cloud service that helps developers create applications such as mobile applications with minimum effort. Built.io is very similar to IFTTT and Zapier but offers advanced functionality.

Cisco Spark : App-centric, cloud-based service that provides a complete collaboration suite for teams to create, meet, message, call, whiteboard, and share, regardless of whether they're together or apart - in one continuous workstream before, during, and after meetings. It is built to help teams work seamlessly. It is simple, secure, complete, and open, and provides a space for people to work better. The core capabilities of Cisco Spark are meetings, messaging, and calling. It can be extended using open RESTful APIs and integrated into other applications or IoT systems.

Fog Computing Model

A fog computing model identifies a distributed computing infrastructure closer to the network edge. It enables edge devices to run applications locally and make immediate decisions. This reduces the data burden on networks as raw data does not need to be sent over network connections. It enhances resiliency by allowing IoT devices to operate when the Internet connection is lost. It also enhances security by keeping sensitive data from being transported beyond the edge where it is needed.

Fog computing extends cloud connectivity closer to the edge. It enables end devices, such as smart meters, industrial sensors, robotic machines, and others, to connect to a local integrated computing, networking, and storage system.

Fog computing includes a combination of hardware and software solutions. Some fog computing platforms support a special operating system called Cisco IOx. This operating system essentially combines Cisco IOS and open source Linux. This enables an IoT router to run IOS and a Linux-based Fog application without having to interact with the cloud.

All fog applications monitor or analyze real-time data from network-connected things and then take action such as locking a door, changing equipment settings, applying the brakes on a train, zooming in with a video camera, opening a valve in response to a pressure reading, creating a bar chart, or sending an alert to a technician to make a preventive repair. The action can involve machine-to-machine (M2M) communications and machine-to-people (M2P) interaction.

Consider a smart traffic light. The traffic light interacts locally with a number of sensors that can detect the presence of pedestrians and bikers, and measure the distance and speed of approaching vehicles. The traffic light also interacts with neighboring lights providing a coordinated effort. Based on this information, the smart light sends warning signals to approaching vehicles and modifies its own cycle to prevent accidents. The data collected by the smart traffic light system is processed locally to do real-time analytics. Re-coordinating with neighboring smart traffic light systems in the Fog allows for any modification of the cycle. For example, it can change the timing of the cycles in response to road conditions or traffic patterns. The data from clusters of smart traffic light systems is sent to the cloud to analyze long-term traffic patterns.

Cisco predicts that 40% of IoT-created data will be processed in the fog by 2018.

Data in Motion and Data at Rest

Simply put, **data in motion** is a term used to refer to the process of extracting value from data while it is being generated. This data may or may not eventually be stored. It is possible to think of data in motion as telling a story as it happens. On the other hand, **data at rest** is data that has been stored.

A variety of industries that rely on extracting value from data before it is stored make use of data in motion. This includes retail, healthcare, manufacturing, energy production, public sector, and service provider markets. With the right infrastructure, data in motion becomes faster and cheaper to use than data at rest because data in motion is easier to locate, and it does not need to be stored.

Because of the vast amount of data that is produced each day, it is no longer feasible to duplicate and store all that data in a centralized data warehouse. Emerging device implementations include a large number of sensors capturing and processing data. Decisions and actions need to take place at the edge, where and when the data is created. With edge nodes gaining more processing power and becoming more context-aware, it is now possible to bring intelligence and analytic algorithms close to the source of the data. In this case, data in motion stays where it is created and presents insights in real time, prompting better, faster decisions.

Click Play in the figure to view the Cisco vision of data in motion.

Cisco NETACAD Connecting Things Chapter 4

It is All About the Data!

Data has become more and more important in business and everyday life. This exponential growth of data has created a new area of interest in technology and business called "big data". In general, big data is data that is so vast and complex that it becomes difficult to store, process, and analyze using traditional data storage and analytics applications.

Big Data is typically characterized in three dimensions: volume, velocity, and variety.

Volume describes the amount of data being transported and stored. The current challenge is to discover ways to most efficiently process the increasing amounts of data, which is predicted to grow 50 times by 2020, to 35 zettabytes.

Velocity describes the rate at which this data is generated. For example, the data generated by a billion shares sold on the New York Stock Exchange cannot just be stored for later analysis. The network infrastructure must be able to immediately respond to the demands of applications accessing and streaming the data.

Variety describes the type of data, which is rarely in a state that is perfectly ready for processing and analysis. A large contributor to big data is unstructured data (application log files, pictures, videos, etc.), which is estimated to represent anywhere from 70 to 90% of world data.

Data that is high in one or more of the 3 V's creates a big data situation.

The characteristics of big data require drastic changes in the way it is supported. The computing platforms must be able to process it; the network must be able to transport it; the storage systems must be able to store and retrieve it; and security measures must be taken to protect it.

Data is very valuable; consequently, it is the main driver behind advancements in technology. Big Data has driven the creation of many new approaches to storage and computing. Examples of open source projects that deal with various aspects of storing, computing, and transmitting big data sets are Apache Hadoop, Spark, Cassandra, and Kafka.

Data that is high in one or more of the 3 V's creates a big data situation.

The characteristics of big data require drastic changes in the way it is supported. The computing platforms must be able to process it; the network must be able to transport it; the storage systems must be able to store and retrieve it; and security measures must be taken to protect it.

Data Transmission

IoT devices are often small, inexpensive devices, with little to no security. Although such devices are computers, they rely on constrained memory and computing resources and may not support complex and evolving security algorithms. Modern encryption algorithms may require more processing power than what is available in the IoT device. In addition to physical security, the IoT device must be able to protect its own firmware and the data it transmits. If data is not properly secured through encryption, it can be intercepted, captured or manipulated while in transit. Any of these actions may compromise the confidence of the system and make the data unreliable.

To mitigate this problem, ensure that IoT devices are running the latest version of their firmware and protocols. Also ensure that any communication is done using protocols that provide secure encryption by default. The encryption algorithm must be strong, with older algorithms tending to present exploitable weaknesses. Regardless of the encryption method chosen, make sure all endpoints agree on the most secure parameters available. A common attack is to trick devices to agree on sub-optimal security parameters under which the connection can be exploited. It is also important to use and verify digital certificates. This is often a challenge with small IoT devices because of their limited memory and CPU capacity.

Servers and cloud endpoints should also be secured and use strong encryption algorithms before communicating with IoT devices. If the IoT device relies on an intermediary device such as a gateway or controller, this intermediary device must also use strong encryption. Naturally, intermediary devices should also be kept up to date with the latest software to keep the device from becoming the weak link that breaks the chain.