The Internet of Things: Network and Security Architecture

by William Stallings, Independent Consultant

The *Internet of Things* (IoT) is the latest development in the long and continuing revolution of computing and communications. Its size, ubiquity, and influence on everyday lives, business, and government dwarf any technical advance that has gone before. IoT is a term that refers to the expanding interconnection of smart devices—ranging from appliances to tiny sensors. A dominant theme is the embedding of short-range mobile transceivers into a wide array of gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves. The Internet now supports the interconnection of billions of industrial and personal objects, usually through cloud systems. The objects deliver sensor information, act on their environment, and in some cases modify themselves, to create overall management of a larger system, like a factory or city[1].

The "things" in IoT are primarily deeply embedded devices, characterized by narrow bandwidth, low-repetition data capture, low-volume data usage. These devices communicate with each other and provide data via user interfaces. Some embedded appliances in the IoT, such as high-resolution video security cameras, video *Voice over IP* (VoIP) phones, and a handful of others, require high-bandwidth streaming capabilities. But countless products simply require packets of data to be intermittently delivered.

This article provides an overview of IoT, and then looks at IoT network and security architectures that will help guide the design, implementation, and deployment of IoT.

Background

The evolving Internet involves billions of objects that use standard communications architectures to provide services to end users. This evolution provides new interactions between the physical world and computing, digital content, analysis, applications, and services. The resulting IoT provides unprecedented opportunities for users, manufacturers, and service providers in a wide variety of sectors. Areas that will benefit from IoT data collection, analysis, and automation capabilities include health and fitness, healthcare, home monitoring and automation, energy savings and smart grid, farming, transportation, environmental monitoring, inventory and product management, security, surveillance, education, and many others.

Technology development is occurring in many areas. Not surprisingly, wireless networking research is being conducted and actually has been conducted for quite a while now, but under previous titles such as mobile computing, pervasive computing, wireless sensor networks, and cyber-physical systems.

Many proposals and products have been developed for low-power protocols, security and privacy, addressing, low-cost radios, energy-efficient schemes for long battery life, and reliability for networks of unreliable and intermittently sleeping nodes. These wireless developments are crucial for the growth of IoT. In addition, areas of development have also involved giving IoT devices social networking capabilities, taking advantage of machine-to-machine communications, storing and processing large amounts of real-time data, and application programming to provide end users with intelligent and useful interfaces to these devices and data.

Many have provided a vision for the IoT. Stankovic[2] suggests personal benefits such as digitizing daily life activities; patches of bionic skin to communicate with surrounding smart spaces for improved comfort, health, and safety; and smart watches and body nodes that optimize access to city services. Citywide benefits could include efficient, delay-free transportation with no traffic lights and 3-D transportation vehicles. Smart buildings could not only control energy and security, but also support health and wellness activities. In the same ways people have been provided new ways of accessing the world through smartphones, the IoT will create a new paradigm in the ways we have continuous access to needed information and services.

Cisco estimates that over the next decade the value at stake (net profit) for the IoT economy is $14.4 trillion[3]. The company's research indicates that five main drivers of this value are at stake:

- *Asset use* ($2.5 trillion): IoT reduces selling, general, and administrative expenses and cost of goods sold by improving business-process execution and capital efficiency.
- *Employee productivity* ($2.5 trillion): IoT creates labor efficiencies that result in fewer or more productive man-hours.
- *Supply chain and logistics* ($2.7 trillion): IoT eliminates waste and improves process efficiencies.
- *Customer experience* ($3.7 trillion): IoT increases customer lifetime value and grows market share by adding more customers.
- *Innovation, including reducing time to market* ($3.0 trillion): IoT increases the return on R&D investments, reduces time to market, and creates additional revenue streams from new business models and opportunities.

Similarly, a 2015 report from McKinsey Global Institute[4] estimates that the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion per year by 2025. On the top end, the value of this impact—including consumer surplus—would be equivalent to about 11 percent of the world economy in 2025.

The Scope of the Internet of Things

The *Telecommunication Standardization Sector of the International Telecommunication Union* (ITU-T) has published Recommendation Y.2060, entitled "Overview of the Internet of Things."[5] The document provides the following definitions that suggest the scope of IoT:

- *Internet of Things* (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.
- *Thing:* With regard to the Internet of Things, this is an object of the physical world (*physical things*) or the information world (*virtual things*), which is capable of being identified and integrated into communication networks.
- *Device:* With regard to the Internet of Things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage, and data processing.

Most of the literature views the IoT as involving intercommunicating smart objects. Recommendation Y.2060 extends this concept to include virtual things, a topic examined subsequently. Recommendation Y.2060 characterizes the IoT as adding the dimension "Any THING communication" to the information and communication technologies that already provide "any TIME" and "any PLACE" communication (Figure 1).

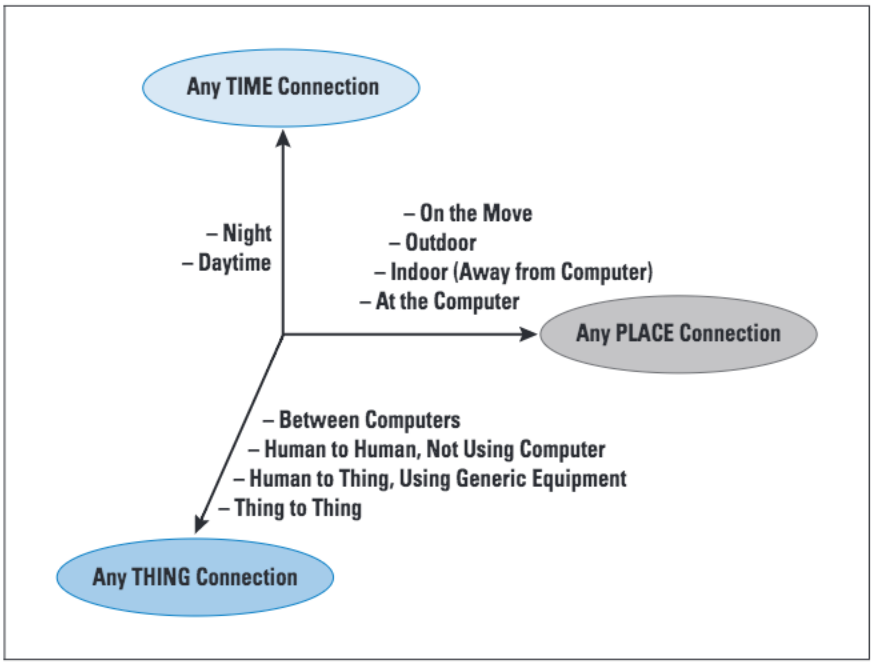


Figure 1: The New Dimension Introduced in the Internet of Things

In the book *Designing the Internet of Things*[6], the elements of the IoT are condensed into a simple equation:

Physical Objects + Controllers, Sensors, Actuators + Internet = IoT

This equation neatly captures the essence of the Internet of Things. An instance of the IoT consists of a collection of physical objects, each of which:

- Contains a microcontroller that provides intelligence;
- Contains a sensor that measures some physical parameter and/or an actuator that acts on some physical parameter;
- Provides a means of communicating via the Internet or some other network.

One item not covered in the equation, and referred to in the Y.2060 definition, is a means of identification of an individual thing, usually referred to as a tag.

Note that although the phrase *the Internet of Things* is always used in the literature, a more accurate description would be an *Internet of Things*, or *a Network of Things*. A smart-home installation, for example, consists of numerous things in the home that are interconnected via Wi-Fi or Bluetooth with some central controller. In a factory or farm setting, a network of things may be enabling enterprise applications to interact with the environment and run applications to exploit the network of things. In these examples, remote access over the Internet is usually, but not invariably, available. Whether or not such Internet connection is available, the collection of smart objects at a site, plus any other local compute and storage devices, can be characterized as a network or an internet of things.

Table 1, on page 6, based on a graphic from Beecham Research[7], gives an idea of the scope of IoT.

IoT Interoperability Standards

In the near term, disparate islands of solutions are likely to outpace deployment of interoperable standards-based solutions for IoT. This situation is common when any new technology or application area emerges. For example, Sutaria and Govindachari[8] point out that two characteristics of networked IoT devices that pose challenges are the presence of low-power devices (which need to function for months or years without power recharge) and frequent data exchanges over lossy networks. Existing Internet standard protocols are suboptimal in this context. In a broader sense, there is a mismatch between the vast number of devices generating data at a rapid rate over a dispersed area and using a variety of network technologies and cloud-based systems that store vast amounts of data in a small number of locations with a relatively slow rate of data update. Integrating these two classes of systems to meet user needs requires specific protocol capabilities along the whole network/protocol architecture, from physical through middleware to application levels.

Table 1: The Internet of Things

Service Sectors	Application Groups	Locations	Example Devices
IT and Networks	Public	Services, e-commerce, data centers, mobile carriers, fixed carriers, ISPs	Servers, storage, PCs, routers, switches, PBXs
	Enterprise	IT/data center, office, private nets	
Security/Public Safety	Surveillance Equipment, Tracking	Radar/satellite, military security, unmanned, weapons, vehicles, ships, aircraft, gear	Tanks, fighter jets, battlefield comms, jeeps
	Public Infrastructure	Human, animal, postal, food/health, packaging, baggage, water treatment, building environmental, general environmental	Cars, breakdown-lane worker, homeland security, fire, environmental monitor
	Emergency Services	Equipment and personnel, police, fire, regulatory	Ambulances, public security vehicles
Retail	Specialty	Fuel stations, gaming, bowling, cinema, discos, special events	POS terminals, tags, cash registers, vending machines, signs
	Hospitality	Hotels, restaurants, bars, cafes, clubs	
	Stores	Supermarkets, shopping centers, single sites, distribution centers	
Transportation	Non-vehicular	Air, rail, marine	Vehicles, lights, ships, planes, signage, tolls
	Vehicles	Consumer, commercial, construction, off-road	
	Transportation Systems	Tolls, traffic management, navigation	
Industrial	Distribution	Pipelines, materials handling, conveyance	Pumps, valves, vats, conveyers, pipelines, motors, drives, converting, fabrication, assembly/ packing, vessels, tanks
	Converting, Discrete	Metals, paper, rubber, plastic, metalworking, electronics assembly, test	
	Fluid/Processes	Petro-chemical, hydrocarbon, food, beverage	
	Resource Automation	Mining, irrigation, agricultural, woodland	
Healthcare and Life Science	Care	Hospital, ER, mobile PoC, clinic, labs, doctor office	MRIs, PDAs, implants, surgical equipment, pumps, monitors, telemedicine
	In-vivo, Home	Implants, home monitoring systems	
	Research	Drug discovery, diagnostics, labs	
Consumer and Home	Infrastructure	Wiring, network access, energy management	Digital camera, power systems, dishwashers, eReaders, desktop computers, washer/dryer, meters, lights, TVs, MP3, games console, lighting, alarms
	Awareness and Safety	Security/alert, fire safety, environmental safety, elderly, children, power protection	
	Convenience and Entertainment	HVAC/climate, lighting, appliance, entertainment	
Energy	Supply/Demand	Power generation, transportation and distribution, low voltage, power quality, energy management	Turbines, windmills, UPS, batteries, generators, meters, drills, fuel cells
	Alternative	Solar, wind, co-generation, electro-chemical	
	Oil/Gas	Rigs, derricks, well heads, pumps, pipelines	
Buildings	Commercial, Institutional	Office, education, retail, hospitality, healthcare, airports, stadiums	HVAC, transport, fire and safety, lighting, security, access
	Industrial	Process, clean room, campus	

To address these issues, several industry bodies and standards forums are working on extending or adopting the Internet protocols to the IoT devices. To provide for a common frame to reference and categorize needed functions and their location in the protocol stack, several of these groups are also addressing the issue of a formal architecture for IoT. While existing standards and the Internet make IoT possible, a suite of widely expected new standards that adapt or augment existing ones for IoT is likely not possible in the near term. Like many other developments made possible by the Internet, IoT will evolve in the wild for a while and pass through Darwinistic processes, with sensible technologies and protocol mechanisms gradually becoming visible. In this article, we look at two efforts at developing overall frameworks that may be useful in this ongoing standardization process.

ITU-T IoT Reference Model

Given the complexity of an IoT, it is useful to have an architecture that specifies the main elements and their interrelationship. An IoT architecture can have the following benefits:

- It provides the IT or network manager with a useful checklist with which to evaluate the functionality and completeness of vendor offerings.
- It provides guidance to developers as to which functions are needed in an IoT and how these functions work together.
- It can serve as a framework for standardization, promoting interoperability and cost reduction.

This section presents an overview of the IoT architecture developed by ITU-T. The next section looks at one developed by *IoT World Forum*. The latter architecture, developed by an industry group, offers a useful alternative framework for understanding the scope and functionality of IoT.

The ITU-T IoT reference model is defined in Recommendation Y.2060[5]. Unlike most of the other IoT reference models and architectural models in the literature, the ITU-T model goes into detail about the actual physical components of the IoT ecosystem. This treatment is useful because it makes visible the elements in the IoT ecosystem that must be interconnected, integrated, managed, and made available to applications. This detailed specification of the ecosystem drives the requirements for the IoT capability.

An important insight the model provides is that the IoT is in fact not a network of physical things. Rather, it is a network of devices that interact with physical things, together with application platforms—such as computers, tablets, and smartphones—that interact with these devices. Thus, we begin our overview of the ITU-T model with a discussion of devices.

Terminology

The following is a list of definitions of key terms used in Recommendation Y.2060:

Communication Network: An infrastructure network that connects devices and applications, such as an IP-based network or internet.

Thing: An object of the physical world (*physical things*) or the information world (*virtual things*) that is capable of being identified and integrated into communication networks.

Device: A piece of equipment with the mandatory capability of communication and the optional capabilities of sensing, actuation, data capture, data storage, and data processing.

Data-carrying Device: A device attached to a physical thing to indirectly connect the physical thing with the communication networks. Active RFID tags are examples.

Data-capturing Device: A reader/writer device with the capability to interact with physical things. The interaction can happen indirectly via data-carrying devices, or directly via data carriers attached to the physical things.

Data Carrier: A battery-free data-carrying object attached to a physical thing that can provide information to a suitable data-capturing device. This category includes bar codes and *Quick Response* (QR) codes attached to physical things.

Sensing Device: A device that detects or measures information related to the surrounding environment and converts it into digital electronic signals.

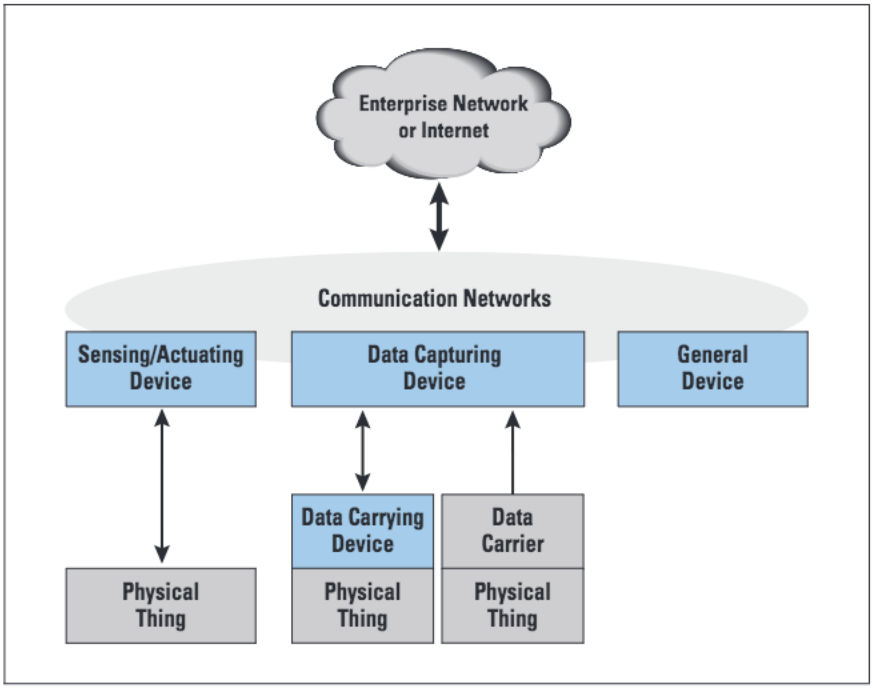
Actuating Device: A device that converts digital electronic signals from the information networks into operations.

General Device: A general device that has embedded processing and communication capabilities and may communicate with the communication networks via wired or wireless technologies. General devices include equipment and appliances for different IoT application domains, such as industrial machines, home electrical appliances, and smartphones.

Gateway: A unit in the IoT that interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

The unique aspect of an IoT, compared to other network systems, of course, is the presence of numerous physical things and devices other than computing or data processing devices. Figure 2, adapted from one in Recommendation Y.2060, shows the types of devices in the ITU-T model. The model views an IoT as functioning as a network of devices that are tightly coupled with things. Sensors and actuators interact with physical things in the environment. Data-capturing devices read data from and/or write data to physical things via interaction with a data-carrying device or a data carrier attached or associated in some way with a physical object.

Figure 2: Types of Devices and Their Relationship with Physical Things



The model makes a distinction between data-carrying devices and data carriers. A data-carrying device is a device in the Recommendation Y.2060 sense. A device at minimum is capable of communication and may include other electronic capabilities. An example of a data-carrying device is an RFID tag. By contrast, a data carrier is an element attached to a physical thing for the purpose of identification or providing some other sort of information.

Y.2060 notes that technologies used for interaction between data-capturing devices and data-carrying devices or data carriers include radio frequency, infrared, optical, and galvanic driving. Examples of each include:

- *Radio Frequency:* A *Radio-Frequency Identification* (RFID) tag is an example.
- *Infrared:* Infrared badges are used in military, hospital, and other settings where the location and movement of personnel need to be tracked. Examples include infrared reflective patches used by the military and battery-operated badges that emit identifying information. The latter can include a button that must be pressed so that the badge can be used as a means of passing through a portal, and a badge that automatically repeats the signal as a means of tracking personnel. Remote-control devices used in the home or other settings to control electronic devices can also easily be incorporated into an IoT.
- *Optical:* Bar codes and QR codes are examples of identifying data carriers that can be read optically.

- *Galvanic Driving:* An example is implanted medical devices that use the conductive properties of the body[9]. In implant-to-surface communication, galvanic coupling sends signals from an implanted device to electrodes on the skin. This scheme uses very little power and reduces the size and complexity of the implanted device.

The final type of device shown in Figure 2 is the general device. These devices have processing and communications capabilities that can be incorporated into an IoT. A good example is smart-home technology that can integrate virtually every device in the home into a network for central or remote control.

Figure 3 provides an overview of the elements of interest in an IoT. The various ways that physical devices can be connected are shown on the left side of the figure. It is assumed that one or multiple networks support communication among the devices.

Figure 3: Technical Overview of the IoT (Recommendation Y.2060)

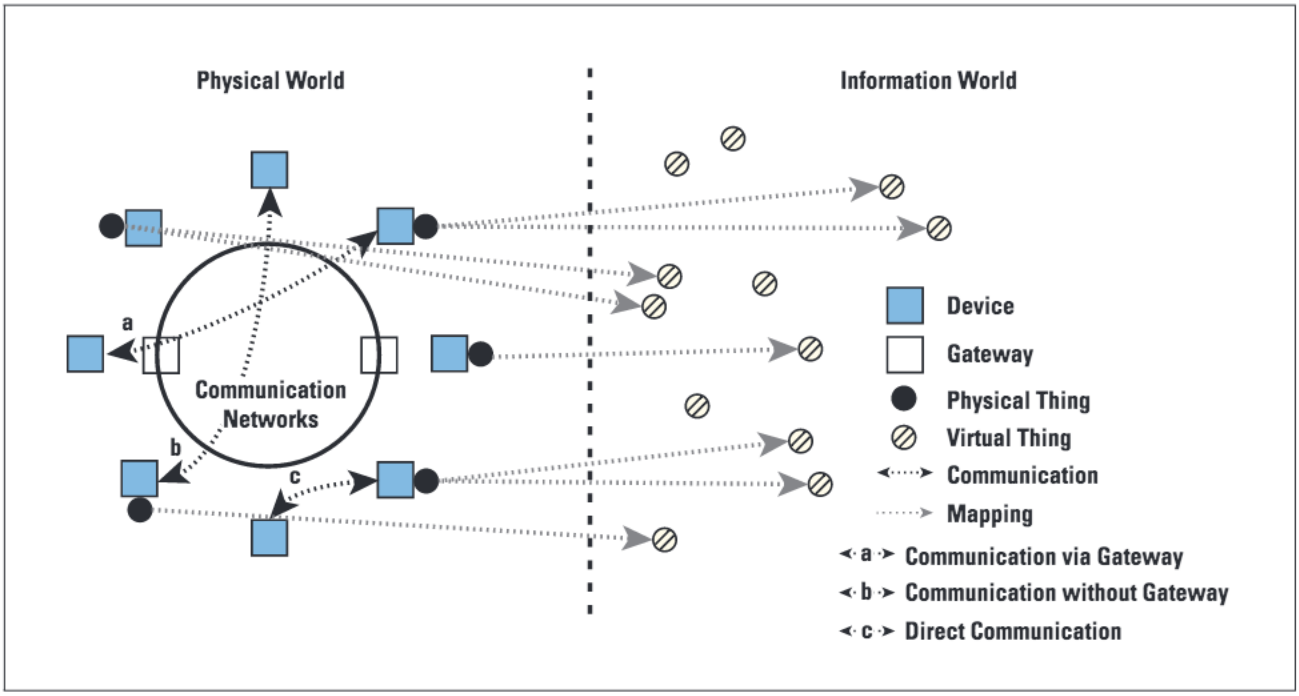


Figure 3 introduces one additional IoT-related device: the *gateway*. At minimum, a gateway functions as a protocol translator. Gateways address one of the greatest challenges in designing an IoT, which is connectivity, both among devices and between devices and the Internet or enterprise network. Smart devices support a wide variety of wireless and wired transmission technologies and networking protocols. Further, these devices typically have limited processing capability.

Recommendation Y.2067[10] lays out the requirements for IoT gateways, which generally fall into three categories:

- The gateway supports a variety of device access technologies, enabling devices to communicate with each other and across an Internet or enterprise network with IoT applications. The access schemes could include, for example, ZigBee, Bluetooth, and Wi-Fi.
- The gateway supports the necessary networking technologies for both local and wide-area networking. These technologies could include Ethernet and Wi-Fi on the premises, and cellular, Ethernet, DSL, and cable access to the Internet and wide-area enterprise networks.
- The gateway supports interaction with application, network management, and security functions.

The first two requirements involve protocol translation between different network technologies and protocol suites. The third requirement is generally referred to as an *IoT agent* function. In essence, the IoT agent provides higher-level functionality on behalf of IoT devices, such as organizing and/or summarizing data from multiple devices to pass on to IoT applications, implementing security protocols and functions, and interacting with network management systems.

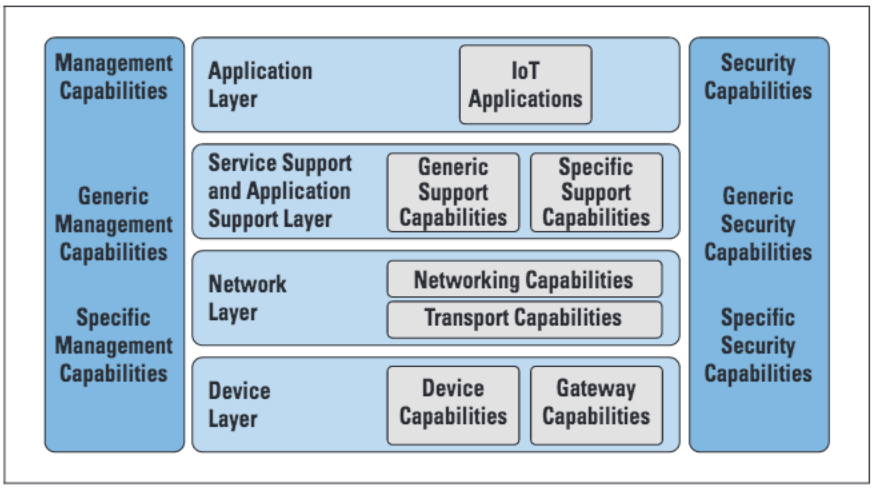
At this point, it should be noted that the term *Communication Network* is not directly defined in the Y.206x series of IoT standards. The communication network or networks support(s) communication among devices and may directly support application platforms. This may be the extent of a small IoT, such as a home network of smart devices. More generally, the device network(s) connect to enterprise networks or the Internet for communication with systems that host apps and servers that host databases related to the IoT.

We can now return to the left side of Figure 3, which illustrates the communication possibilities among devices. The first possibility is for communication between devices via the gateway. For example, a sensor or actuator with Bluetooth capability could communicate with a data-capturing device or general device that uses Wi-Fi by means of the gateway. The second possibility is communication across the communication network without a gateway. For example, all of the devices in a smart-home network may use Bluetooth and could be managed from a Bluetooth-enabled computer, tablet, or smartphone. The third possibility is devices that communicate directly with each other through a separate local network and then (not shown in the figure) communicate through the communication network via a local network gateway. An example of this third possibility follows: Numerous low-power sensor devices could be deployed in an extended area, such as farmland or a factory. These devices could communicate with one another to pass data on toward a device connected to a gateway to the communication network.

The right side of Figure 3 emphasizes that each physical thing in an IoT may be represented in the information world by one or more virtual things, but a virtual thing can also exist without any associated physical thing. Physical things are mapped to virtual things stored in databases and other data structures. Applications process and deal with virtual things.

Figure 4 depicts the ITU-T IoT reference model, which consists of four layers as well as management capabilities and security capabilities that apply across layers. We have so far been considering the device layer. In terms of communications functionality, the device layer includes, roughly, the OSI physical and data link layers. We now look at the other layers.

Figure 4: ITU-T Recommendation Y.2060 IoT Reference Model



The *Network Layer* performs two basic functions. Networking capabilities refer to the interconnection of devices and gateways. Transport capabilities refer to the transport of IoT service- and application-specific information as well as IoT-related control and management information. Roughly, these capabilities correspond to those of the OSI network and transport layers.

The *Service Support and Application Support Layer* provides capabilities that applications use. Many different applications can use generic support capabilities. Examples include common data processing and database management capabilities. Specific support capabilities are those that cater for the requirements of a specific subset of IoT applications.

The *Application Layer* consists of all the applications that interact with IoT devices.

The *Management Capabilities Layer* covers the traditional network-oriented management functions of fault, configuration, accounting, and performance management.

Recommendation Y.2060 lists the following as examples of generic management capabilities:

- *Device Management:* Examples include device discovery, authentication, remote device activation and de-activation, configuration, diagnostics, firmware and/or software updating, and device working-status management.
- *Local Network Topology Management:* An example is network configuration management.
- *Traffic and Congestion Management:* Examples include the detection of network overflow conditions and the implementation of resource reservation for time- and/or life-critical data flows.

Specific management capabilities are tailored to specific classes of applications. An example is smart-grid power-transmission-line monitoring.

The *Security Capabilities Layer* includes generic security capabilities that are independent of applications. Y.2060 lists the following as examples of generic security capabilities:

- *Application Layer:* authorization, authentication, and application data confidentiality and integrity protection, privacy protection, security audit, and anti-virus.
- *Network Layer:* authorization, authentication, user data, and signaling data confidentiality, and signaling integrity protection.
- *Device Layer:* authentication, authorization, device-integrity validation, access control, data confidentiality, and integrity protection.

Specific security capabilities relate to specific application requirements, such as mobile payment security requirements.

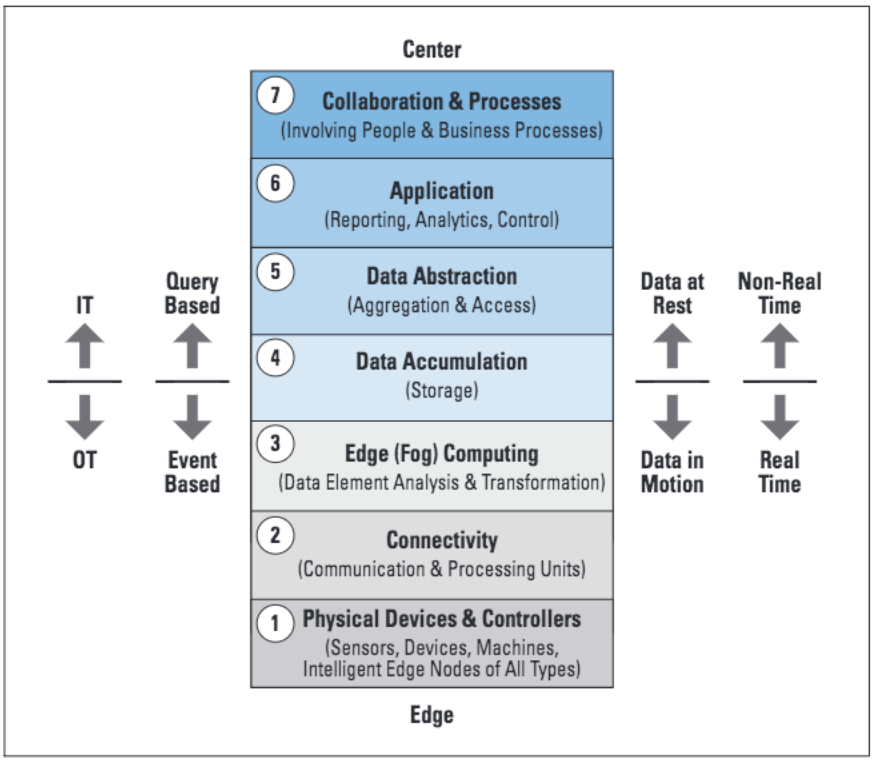
IoT World Forum Reference Model

The *IoT World Forum* (IWF) is an industry-sponsored annual event that brings together representatives of business, government, and academia to promote the market adoption of IoT. The IoT World Forum *Architecture Committee,* made up of industry leaders including IBM, Intel, and Cisco, released an IoT reference model in October 2014. This model serves as a common framework to help the industry accelerate IoT deployments. The reference model is intended to foster collaboration and encourage the development of replicable deployment models.

This reference model is a useful complement to the ITU-T reference model. The ITU-T documents focus on the device and gateway level with only a broad depiction of the upper layers. Indeed, Recommendation Y.2060 describes the application layer with a single sentence. The ITU-T Recommendation Y.206x series seems most concerned with defining a framework to support development of standards for interaction with IoT devices.

The IWF is concerned with the broader issue of developing the applications, middleware, and support functions for an enterprise-based IoT. Figure 5 depicts the seven-level model.

Figure 5: IoT World Forum Reference Model



The white paper on the IWF model issued by Cisco[11] indicates that the model is designed to have the following characteristics:

- *Simplifies:* It helps break down complex systems so that each part is more understandable.
- *Clarifies:* It provides additional information to precisely identify levels of the IoT and to establish common terminology.
- *Identifies:* It identifies where specific types of processing are optimized across different parts of the system.
- *Standardizes:* It provides a first step in enabling vendors to create IoT products that work with each other.
- *Organizes:* It makes the IoT real and approachable, instead of simply conceptual.

Level 1 comprises physical devices and controllers that might control multiple devices. Level 1 of the IWF model corresponds approximately to the device level of the ITU-T model (Figure 4). As with the ITU-T model, the elements at this level are not physical things as such, but rather devices that interact with physical things, such as sensors and actuators. Among the capabilities that devices may have are analog-to-digital and digital-to-analog conversion, data generation, and the ability to be queried and/or controlled remotely.

From a logical point of view, this level enables communication between devices and between devices and the low-level processing that occurs at level 3. From a physical point of view, this level consists of networking devices such as routers, switches, gateways, and firewalls that are used to construct local and wide-area networks and provide Internet connectivity. This level enables devices to communicate with one another and to communicate, via the upper logical levels, with application platforms such as computers, remote-control devices, and smartphones.

Level 2 of the IWF model corresponds approximately to the network level of the ITU-T model. The main difference is that the IWF model includes gateways in level 2, whereas the ITU-T model puts the gateway at level 1. Because the gateway is a networking and connectivity device, its placement at level 2 seems to make more sense.

In many IoT deployments, massive amounts of data may be generated by a distributed network of sensors. For example, offshore oil fields and refineries can generate a terabyte of data per day. An airplane can create multiple terabytes of data per hour. Rather than store all of that data permanently (or at least for a long period) in central storage accessible to IoT applications, it is often desirable to do as much data processing close to the sensors as possible. Thus, the purpose of the edge computing level is to convert network data flows into information that is suitable for storage and higher-level processing. Processing elements at these levels may deal with high volumes of data and perform data-transformation operations, resulting in the storage of much lower volumes of data. The Cisco white paper on the IWF model[11] lists the following examples of edge computing operations:

- *Evaluation:* Evaluating data for criteria as to whether it should be processed at a higher level.
- *Formatting:* Reformatting data for consistent higher-level processing.
- *Expanding/decoding:* Handling cryptic data with additional context (such as the origin).
- *Distillation/reduction:* Reducing and/or summarizing data to minimize the impact of data and traffic on the network and higher-level processing systems.
- *Assessment:* Determining whether data represents a threshold or alert; this process could include redirecting data to additional destinations.

Processing elements at this level corresponds to general devices in the ITU-T model (Figure 2). Generally, they are deployed physically near the edge of the IoT network; that is, near the sensors and other data-generating devices. Thus, some of the basic processing of large volumes of generated data is offloaded and outsourced from IoT application software located at the center.

Processing at the edge computing level is sometimes referred to as *Fog Computing*. Fog computing and fog services are expected to be a distinguishing characteristic of the IoT. Figure 6 illustrates the concept. Fog computing represents an opposite trend in modern networking from cloud computing. With cloud computing, massive, centralized storage and processing resources are made available to distributed customers over cloud networking facilities to a relatively small number of users. With fog computing, massive numbers of individual smart objects are interconnected with fog networking facilities that provide processing and storage resources close to the edge devices in an IoT. Fog computing addresses the challenges raised by the activity of thousands or millions of smart devices, including security, privacy, network-capacity constraints, and latency requirements. The term "Fog Computing" is inspired by the fact that fog tends to hover low to the ground, whereas clouds are high in the sky.

Figure 6: Fog Computing

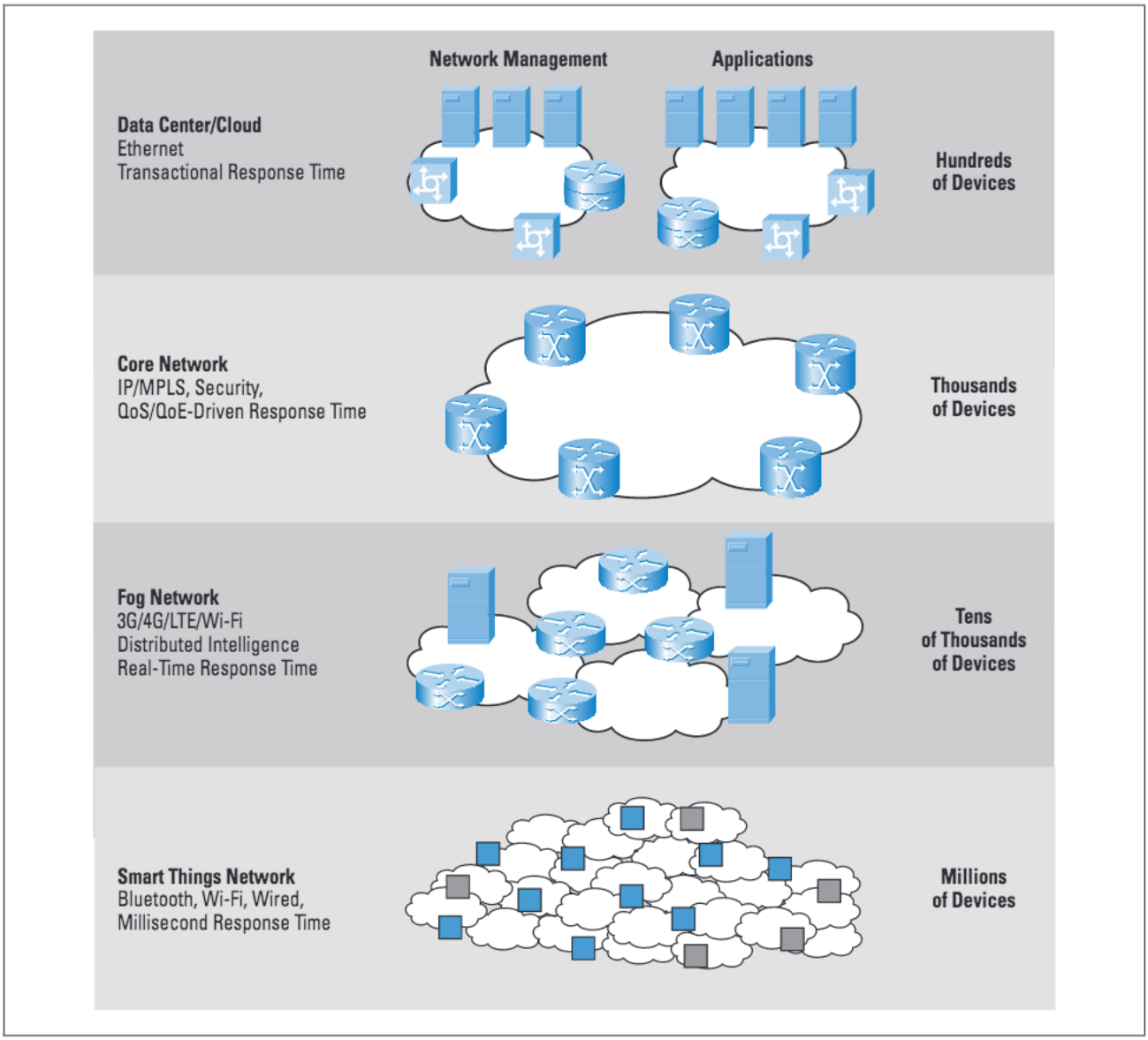


Table 2, based on one in [12], compares cloud and fog computing.

Table 2: Comparison of Cloud and Fog Features

	Cloud	Fog
Location of processing/ storage resources	Center	Edge
Latency	Low to high	Low
Access	Fixed or wireless	Mainly wireless
Support for mobility	Not applicable	Yes
Control	Centralized/hierarchical (full control)	Distributed/hierarchical (partial control)
Service access	Through core	At the edge/on handheld device
Availability	99.99%	Highly volatile/highly redundant
Number of users/devices	Tens/hundreds of millions	Tens of billions
Main content generator	Humans and devices	Devices/sensors
Content generation	Central location	Anywhere
Content consumption	End device	Anywhere
Software virtual infrastructure	Central enterprise servers	User devices

Level 4, the data accumulation level, is where data coming from the numerous devices, and filtered and processed by the edge computing level, is placed in storage that will be accessible by higher levels. This level marks a clear distinction in the design issues, requirements, and method of processing between lower-level (fog) computing and upper-level (typically cloud) computing.

Data moving through a network is referred to as *data in motion*. The rate and organization of the data in motion is determined by the devices generating the data. Data generation is event-driven, either periodically or by an event in the environment. To capture the data and deal with it in some fashion, it is necessary to respond in real time. By contrasts, most applications do not need to process data at network transfer speeds. As a practical matter, neither the cloud network nor the application platforms would be able to keep up with data volume generated by a huge number of IoT devices. Instead, applications deal with *data at rest,* which is data in some readily accessible storage facility. Applications can access the data as needed, on a non-real-time basis. Thus, the upper levels operate on a query or transaction basis, whereas the lower three levels operate on an event basis.

The following are listed as operations performed at the data-accumulation level in [13]:

- Converts data in motion to data at rest
- Converts format from network packets to database relational tables
- Achieves transition from event-based to query-based computing
- Dramatically reduces data through filtering and selective storing

Another way of viewing the data-accumulation level is that it marks the boundary between *Information Technology* (IT), which is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services, and *Operational Technology* (OT), which refers to hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.

The data-accumulation level absorbs large quantities of data and places them in storage, with little or no tailoring to specific applications or groups of applications. Numerous different types of data in varying formats and from heterogeneous processors may be coming up from the edge computing level for storage. The data-abstraction level can aggregate and format this data in ways that make access by applications more manageable and efficient. Tasks involved could include:

- Combining data from multiple sources, including reconciling multiple data formats.
- Performing necessary conversions to provide consistent semantics of data across sources.
- Placing formatted data in an appropriate database; for example, high-volume repetitive data may go into a big data system such as Hadoop. Event data would be steered to a relational database management system, which provides faster query times and an appropriate interface for this type of data.
- Alerting higher-level applications that data is complete or has accumulated to a defined threshold.
- Consolidating data into one place (with ETL (*extract, transform, load*), ELT (*extract, load, transform*), or data replication) or providing access to multiple data stores through data virtualization.
- Protecting data with appropriate authentication and authorization.
- Normalizing or denormalizing and indexing data to provide fast application access.

The application level contains any type of application that uses IoT input or controls IoT devices. Generally, applications interact with level 5 and the data at rest, and so do not have to operate at network speeds. Provision should be available for streamlined operation that allows applications to bypass intermediate layers and interact directly with Layer 3 or even Layer 2. The IWF model does not strictly define applications, considering it beyond the scope of IWT model discussion.

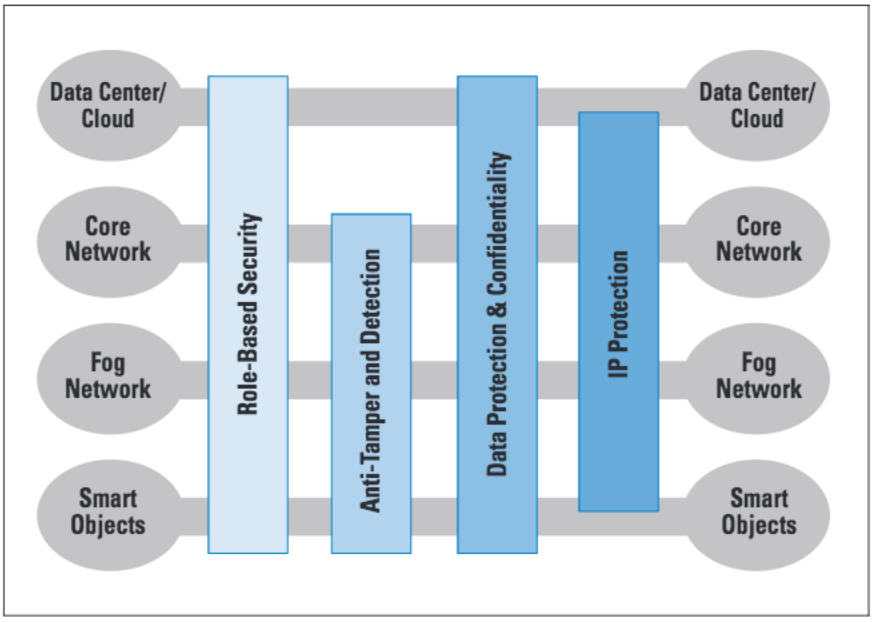
The collaboration and processes level recognizes that people must be able to communicate and collaborate to make an IoT useful. This level may involve multiple applications and exchange of data and control information across the Internet or an enterprise network.

The IWF views the IoT reference model as an industry-accepted framework aimed at standardizing the concepts and terminology associated with IoT. More importantly, the IWF model sets out the functionalities required and concerns that must be addressed before the industry can realize the value of the IoT. This model is useful both for suppliers who develop functional elements within the model and customers for developing their requirements and evaluating vendor offerings.

An IoT Security Framework

Cisco Systems, which has played a lead role in the development of the IoT World Forum Reference Model, has developed a framework for IoT security[13] that serves as a useful complement to the World Forum IoT Reference Model. Figure 7 illustrates the security environment related to the logical structure of an IoT.

Figure 7: IoT Security Environment



The Cisco IoT model is a simplified version of the World Forum IoT Reference Model. It consists of the following levels:

- *Smart Objects/Embedded Systems:* This level consists of sensors, actuators, and other embedded systems at the edge of the network. This part of an IoT is the most vulnerable part. The devices may not be in a physically secure environment and may need to function for years. Availability is certainly of concern. Also network managers need to be concerned about the authenticity and integrity of the data generated by sensors and about protecting actuators and other smart devices from unauthorized use. Privacy and protection from eavesdropping may also be requirements.
- *Fog/Edge Network:* This level is concerned with the wired and wireless interconnection of IoT devices. In addition, a certain amount of data processing and consolidation may be done at this level. A key concern is the wide variety of network technologies and protocols that the various IoT devices use and the need to develop and enforce a uniform security policy.
- *Core Network:* The core network level provides data paths between network center platforms and the IoT devices. The security issues here are those confronted in traditional core networks. However, the vast number of endpoints to interact with and manage creates a substantial security burden.
- *Data Center/Cloud:* This level contains the application, data storage, and network management platforms. IoT does not introduce any new security issues at this level, other than the necessity of dealing with huge numbers of individual endpoints.

Within this four-level architecture, the Cisco model defines four general security capabilities that span multiple levels:

- *Role-Based Security: Role-Based Access Control* (RBAC) systems assign access rights to roles instead of individual users. In turn, users are assigned to different roles, either statically or dynamically, according to their responsibilities. RBAC enjoys widespread commercial use in cloud and enterprise systems and is a well-understood tool that can be used to manage access to IoT devices and the data they generate.
- *Anti-tamper and Detection:* This function is particularly important at the device and fog network levels but also extends to the core network level. All of these levels may involve components that are physically outside the area of the enterprise that is protected by physical security measures.
- *Data Protection and Confidentiality:* These functions extend to all levels of the architecture.
- *Internet Protocol Protection:* Protection of data in motion from eavesdropping and snooping is essential between all levels.

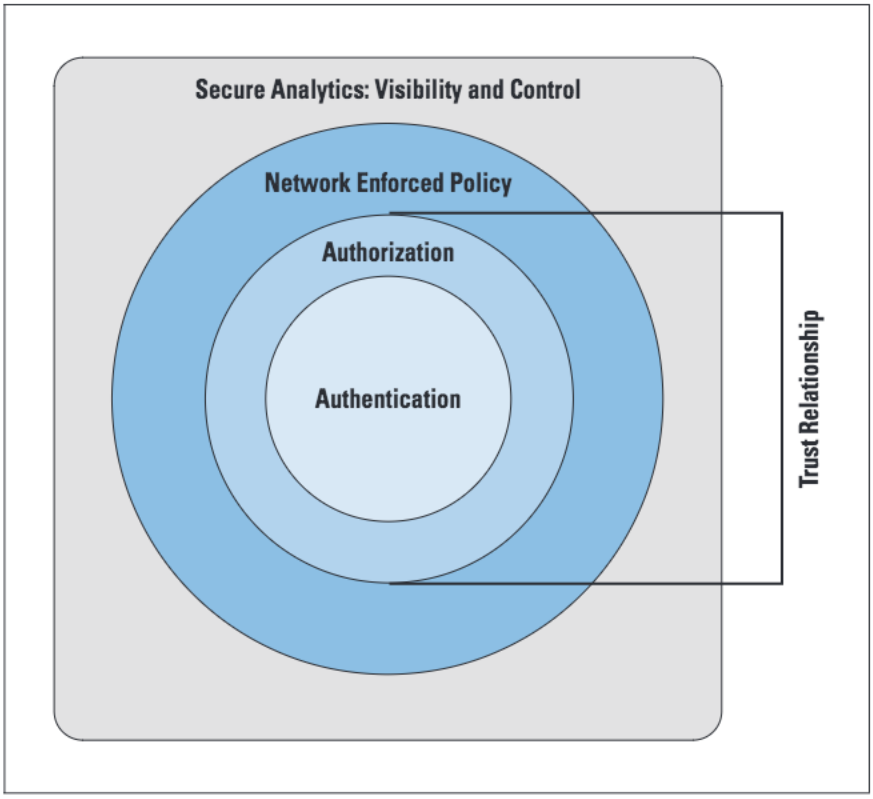
Figure 7, on page 19, maps specific security functional areas across the four layers of the IoT model. The Cisco white paper[13] also proposes a secure IoT framework that defines the components of a security facility for an IoT that encompasses all the levels, as shown in Figure 8 on page 22. The four components follow:

- *Authentication:* This component encompasses the elements that initiate the determination of access by first identifying the IoT devices. In contrast to typical enterprise network devices, which may be identified by a human credential (for example, username and password or token), the IoT endpoints must be fingerprinted by means that do not require human interaction. Such identifiers include RFID, x.509 certificates, or the MAC address of the endpoint.
- *Authorization:* Authorization controls access of a device throughout the network fabric. This element encompasses access control. Together with the authentication layer, it establishes the necessary parameters to enable the exchange of information between devices and between devices and application platforms and enables IoT-related services to be performed.
- *Network Enforced Policy:* This component encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management, or actual data traffic.
- *Secure Analytics, including Visibility and Control:* This component includes all the functions required for central management of IoT devices. It involves, firstly, visibility of IoT devices, meaning simply that central management services are securely aware of the distributed IoT device collection, including identity and attributes of each device. Building on this visibility is the ability to exert control, including configuration, patch updates, and threat countermeasures.

An important concept related to this framework is that of *trust relationship*. In this context, trust relationship refers to the ability of the two partners to an exchange to have confidence in the identity and access rights of the other. The authentication component of the trust framework provides a basic level of trust, which is expanded with the authorization component.

The Cisco white paper[13] gives the example that a car may establish a trust relationship with another car from the same vendor. That trust relationship, however, may allow cars to exchange only their safety capabilities. When a trusted relationship is established between the same car and its dealer's network, the car may be allowed to share additional information such as its odometer reading and last maintenance record.

Figure 8: Secure IoT Framework



Conclusions

According to the McKinsey report cited earlier[4], approximately 40 percent of the total economic value of the IoT is driven by the ability of all the physical devices to talk to each other via computers, that is, interoperability. If interoperability is limited, the IoT might be only a $7 trillion opportunity, whereas widespread interoperability could achieve an IoT value to the global economy of over $11 trillion by 2025. On average, 40 percent of the total value that can be unlocked requires different IoT systems to work together. Table 3, based on the McKinsey report, estimates the percent of economic value that requires interoperability between IoT systems for different sectors.

To achieve the type of interoperability needed to realize these benefits, standards need to be developed at all levels of IoT functionality, from the device layer to the application layer (Figure 4). While such standardization is still in its infancy, the architectural models described here provide a useful framework for future efforts.

Table 3: Value Added by IoT Interoperability

Setting	Value Potential Requiring Interoperability ($ Trillion)	% of Total Value	Examples of How Interoperability Enhancs Value
Factories	1.3	36	Data from different types of equipment used to improve line efficiency
Cities	0.7	43	Video, cellphone data, and vehicle sensors to monitor traffic and optimize flow
Retail	0.7	57	Payment and item-detection system linked for automatic checkout
Work sites	0.5	56	Linking worker and machinery location data to avoid accidents and exposure to chemicals
Vehicles	0.4	44	Equipment usage data for insurance underwriting, maintenance, and presales analytics
Agriculture	0.3	20	Multiple sensor systems used to improve farm management
Outside	0.3	29	Connected navigation between vehicles and between vehicles and GPS/traffic control
Home	0.1	17	Linking chore automation to security and energy system to time usage
Offices	>0.1	30	Data from different building systems and other buildings used to improve security

References

[1] Lake, D., Rayes, A., and Morrow, M., "The Internet of Things," *The Internet Protocol Journal,* Volume 15, No. 3, September 2012.

[2] Stankovic, J., "Research Directions for the Internet of Things," *Internet of Things Journal,* Volume 1, No. 1, 2014.

[3] Cisco Systems, "Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion," White Paper, 2013. **http://www.cisco.com/web/about/ac79/docs/innov/IoT_Economy_Insights.pdf**

[4] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype," June 2015. **http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world**

[5] ITU-T, "Overview of the Internet of Things," Recommendation Y.2060, June 2012.

[6] McEwen, A., and Cassimally, H., *Designing the Internet of Things,* ISBN-13: 978-1118430620, Wiley, 2013.

[7] Beecham Research. "M2M Sector Map," September 2011. `http://www.beechamresearch.com/downloads.aspx?page=2`

[8] Sutaria, R., and Raghunath, G., "Making sense of interoperability: Protocols and Standardization initiatives in IoT," *International Conference on Recent Trends in Communication and Computer Networks – ComNet 2013*, 2013.

[9] Ferguson, J., and Redish, A., "Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body," Expert Review of Medical Devices, Volume 6, No. 4, 2011, `http://www.expert-reviews.com`.

[10] ITU-T, "Common Requirements and Capabilities of a Gateway for Internet of Things Applications," Recommendation Y.2067, June 2014.

[11] Cisco Systems, "The Internet of Things Reference Model," White Paper, 2014. `http://www.iotwf.com/`

[12] Vaquero, L., and Rodero-Merino, L., "Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing," *ACM SIGCOMM Computer Communication Review,* October 2014.

[13] Frahim, J., et al., "Securing the Internet of Things: A Proposed Framework," Cisco White Paper, March 2015.

[14] Douglas Comer, "The ZigBee IP Protocol Stack," *The Internet Protocol Journal,* Volume 17, No. 2, December 2014.

WILLIAM STALLINGS is an independent consultant and author of numerous books on security, computer networking, and computer architecture. His latest book is *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (Pearson, 2016). He maintains a resource site for computer science students and professionals at `ComputerScienceStudent.com` and is on the editorial board of *Cryptologia*. He has a Ph.D. in computer science from M.I.T. He can be reached at `ws@shore.net`