Internet of Things for Telecom Engineers

A Report on Current State and Future Technologies

Based on research compiled from content in the IEEE *Xplore* Digital Library

IEEE

IEEE *Xplore*®
Digital Library

Table of Contents

IEEE Xplore®
Digital Library

A New Era for Telecommunications

> *"Over time, the IoT is expected to have significant home and business applications, to contribute to the quality of life and to grow the world's economy."* [1]

The Internet of Things (IoT) is no longer the future: it is the new reality moving telecommunications forward. The IoT enables physical objects to see, hear, think, and perform jobs by having them "talk" to each other, share information, and coordinate decisions.

The number of internet-enabled objects has surpassed the Earth's population. Today, the IoT connects everything from HVAC thermostats and smart homes to transportation, healthcare, industrial automation, and emergency response equipment. As the prevalence of IoT innovations grow, telecom leaders must embrace the opportunities, and challenges, posed by a more connected future.

The Framework for Connected Technologies

The IoT connects domain-specific applications in vertical markets such as healthcare, industry, and agriculture with application-domain-independent services in horizontal markets such as analytics and network monitoring. These outlying domain-specific applications interact with domain-independent services as shown in [1, Fig.1]. In each domain, sensors and actuators communicate directly with each other.

The communications within each application, and within this center hub, give the Internet of Things the **unprecedented power to improve quality of life and grow the world's economy.**

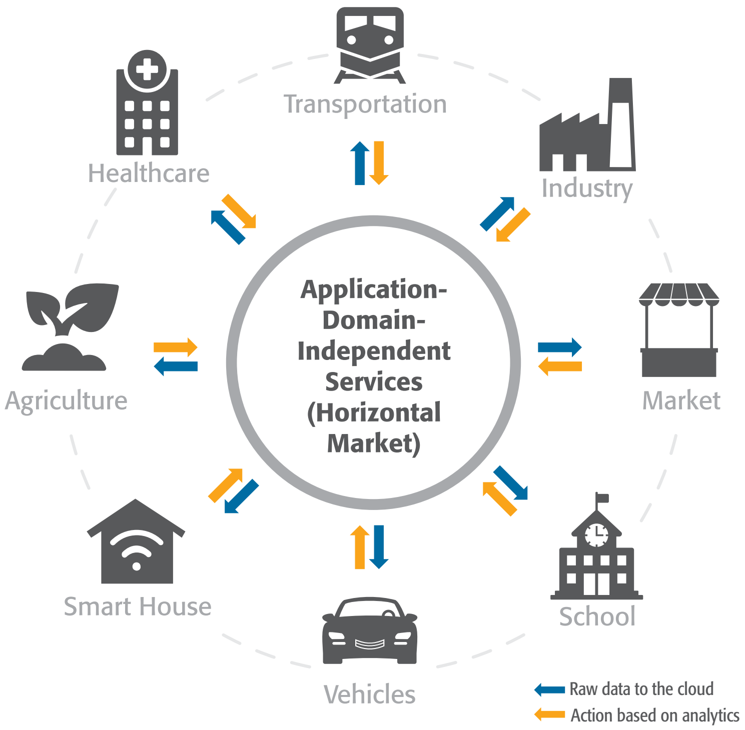


Figure 1. Connected technologies framework

Building a Connected Future for Telecommunications

To realize the potential of the Internet of Things, telecom leaders must:

- Support growth of emerging technologies, innovations, and service applications
- Develop devices that provide availability anywhere and anytime
- Create new protocols for communication compatibility among objects that differ greatly (living things, vehicles, smartphones, appliances, goods, etc.)
- Standardize architecture to accommodate the tremendous number of objects trying to connect to the internet
- Offer larger addressing spaces (e.g., IPv6) to meet customer demand for smart objects
- Increase security and privacy in those technologies
- Improve management and monitoring to ensure cost-efficient, high-quality services

Acknowledgements

This white paper explores current practices and future possibilities for a world securely and completely connected by technology. It is based on research compiled from the following content available in the IEEE *Xplore* digital library; a full citation is available at the end of this white paper. A subscription to IEEE *Xplore* provides full access to those articles and more than four million additional periodicals, conference proceedings, standards, eBooks and online courses. See if your organization qualifies for a free trial by visiting us here: ieee.org/telecom-free-trial

"Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,"
Published in *IEEE Communications Surveys & Tutorials*

"IoT technologies for smart cities,"
Published in *IET Networks*

"Mobile Health (m-Health) System in the Context of IoT,"
Published in the proceedings of the *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*

"Security threats in the application layer in IoT applications," Published in the proceedings of the *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*

"The Internet of Things: Why now, and what's next?,"
Published in *IEEE Consumer Electronics Magazine*

"Security and Privacy for Cloud-Based IoT: Challenges,"
Published in *IEEE Communications Magazine*

"Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things,"
Published in *IEEE Pervasive Computing*

"Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies,"
Published in *IEEE Consumer Electronics Magazine*

"Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches,"
Published in *IEEE Communications Magazine*

About the IEEE Xplore Digital Library

The IEEE *Xplore* digital library is your gateway to trusted technology research—journals, conferences, standards, ebooks, and educational courses—with more than four million articles to help you fuel imagination, build from previous research, and increase productivity.

IEEE *Xplore* opens a world of knowledge from many industries to enable you to improve or discover the next breakthrough. With powerful search tools to help you find only the most relevant research, IEEE *Xplore* delivers the information your company needs to innovate.

> *“In order to realize this potential growth, emerging technologies, innovations and applications need to grow proportionally to match market demands and customer needs.”*[1]

Telecom Opportunities

As the capabilities of the IoT grow, so too will opportunities for providers across industries, including telecommunications. Experts report that scalable, secure solutions represent incredible potential for smart cities connected by the IoT. With 50 billion connected devices expected by 2020, corporations such as Telefónica and SK Telecom, as well as industry groups including GDF SUEZ and Air Liquide, have already invested €100 million to research and deploy IoT technologies in smart cities worldwide [2].

By 2022, projections indicate that 45% of all internet traffic will consist of machine-to-machine (M2M) traffic flows. By 2025, the full global economic impact of the IoT is estimated to be in range of $2.7 trillion to $6.2 trillion [1].

Preparing for Significant Growth in Many Industries

Healthcare applications alone are expected to create about $1.1–$2.5 trillion in global economic growth annually by 2025. Examples include mobile health (m-Health) and telecare delivered via electronic media for efficient medical wellness, prevention, diagnosis, treatment, and monitoring. Such devices transmit and receive data over a wireless network via a unique IP address [3]. On average, these innovations are low cost, low power, small and simple to use. Examples already delivering measurable impact include Bluetooth-compatible smart watches and blood sugar meters.

In manufacturing, advisory resources expect the industrial internet will deliver $1.3 trillion in value by 2020, growing return on investment by 149%. Navigant recently reported that the Building Automation Systems (BAS) market is expected to increase by 60%, from $58.1 billion in 2013 to reach $100.8 billion by 2021.

For telecom organizations, this growth will provide opportunities to connect the energy efficiencies, security, and data protection of modern facilities via optimized networks. Spreading the IoT and related services globally requires internet service providers (ISPs) to provision their networks to provide a high level of service for M2M, person-to-machine (P2M), and person-to-person (P2P) traffic flows [1].

> ***"By 2025, the global economic impact of the IoT is estimated to be $2.7 to $6.2 trillion."*** *[1]*

> “The industrial internet will deliver **$1.3 trillion in value** by 2020, with a **149% return on investment**.”[1]

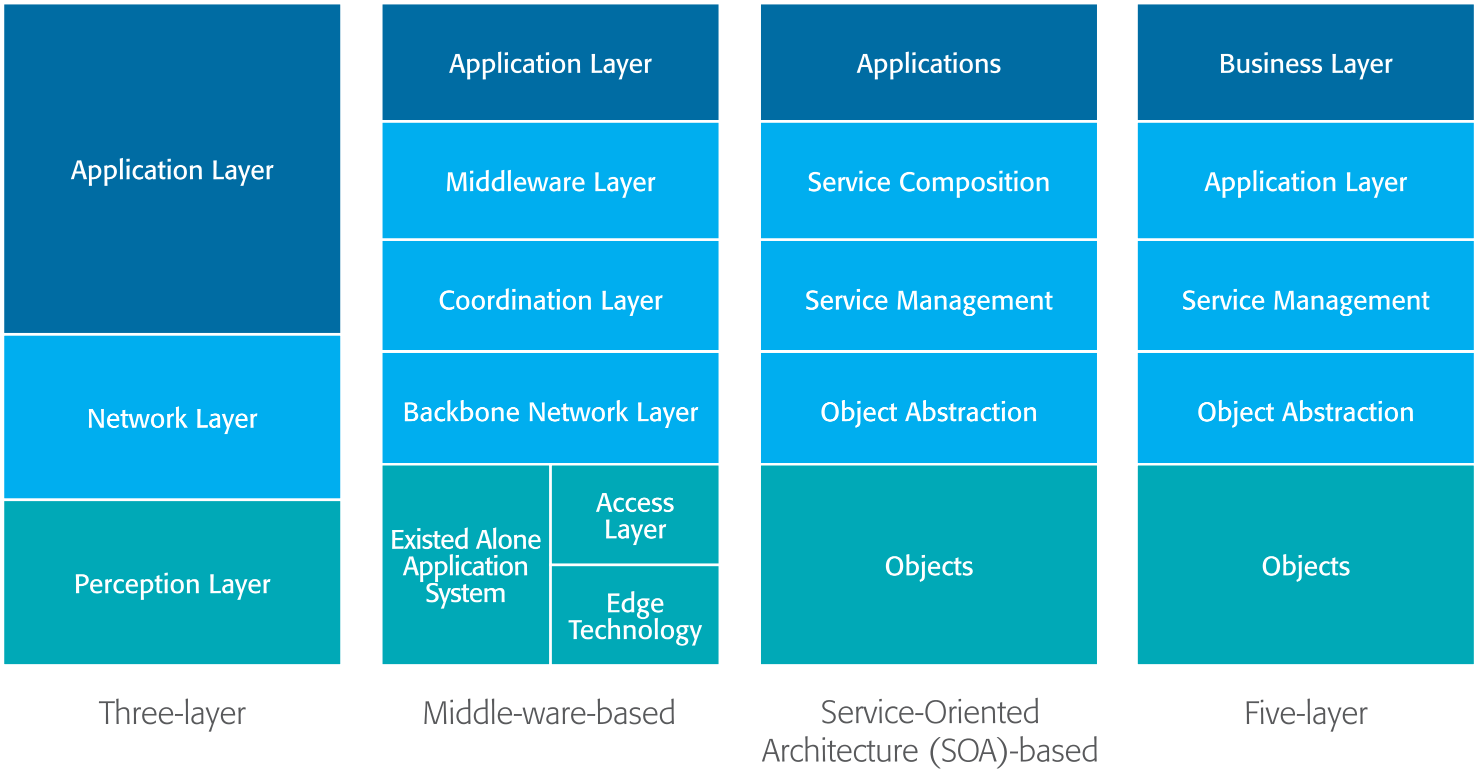
IoT Architecture

> *"…[Architecture] standardization can be seen as a backbone for the IoT to create a competitive environment for companies to deliver quality products." [1]*

As it continues to expand, the IoT will need a flexible, layered architecture to connect billions or trillions of heterogeneous objects via the internet. While projects like IoT-A are tasked with designing a common architecture, a dominant choice has yet to be defined. Most initial models featured a three-layer architecture [1] consisting of the Perception, Network, and Application layers.

At the Perception layer, physical sensors gather and digitize data to be transmitted over secure channels. Next, the Network Layer manages the aggregation, filtering, and routing of data to IoT hubs and smart devices. Finally, the Application delivers data to end-user devices [4]. More recent models have added more abstraction to the IoT architecture. The result is a five-layer framework that relies on the demand and performance of IoT-ready objects and builds upwards illustrated in [1, Fig. 2].

Defining the Layers of the IoT



Three-layer

Application Layer

Network Layer

Perception Layer

Middle-ware-based

Application Layer

Middleware Layer

Coordination Layer

Backbone Network Layer

Existed Alone Application System

Access Layer

Edge Technology

Service-Oriented Architecture (SOA)-based

Applications

Service Composition

Service Management

Object Abstraction

Objects

Five-layer

Business Layer

Application Layer

Service Management

Object Abstraction

Objects

Figure 2. Layers of the IoT

Defining the Layers of the IoT

Objects Layer

Big data created by the IoT begins in this foundational layer, which includes the physical sensors of the IoT that collect and process information. These objects include sensors and actuators for querying location, temperature, weight, motion, vibration, acceleration, humidity, etc.

Object Abstraction Layer

Here, technologies like RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth Low Energy, infrared, and ZigBee transfer data produced in the Objects layer to the Service Management layer. This layer also handles functions like cloud computing and data management processes.

Service Management Layer

In this layer, services are paired with requesters based on addresses and names. Here, IoT application programmers work with a full range of objects from different hardware platforms. The layer also processes received data, makes decisions, and delivers required services over network wire protocols [1].

Application Layer

This layer provides high-quality smart services for smart homes, smart buildings, transportation, industrial automation, as well as smart healthcare services.

Business Layer

This layer manages IoT system activities and services, building business models, graphs, flowcharts, etc. from received data in the Application layer. It also designs, analyzes, implements, evaluates, monitors, and develops IoT system-related elements. The Business layer also supports decision-making processes based on big data analysis [1].

[1, Fig. 3] illustrates where standards, such as key protocols and devices, are engaged in both the three-layer and five-layer architecture of the IoT [1].

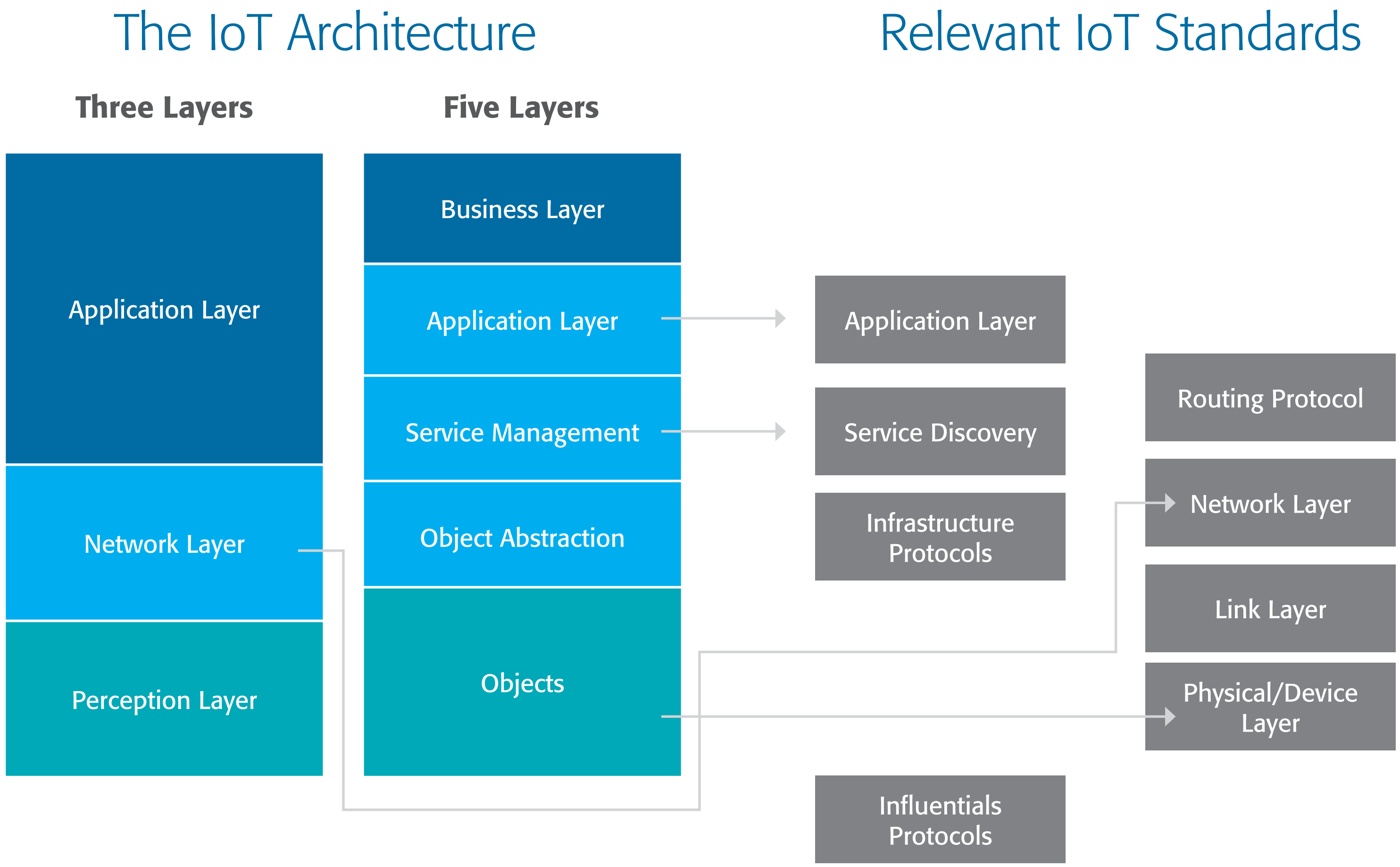


Figure 3. Layers of the IoT

> *“The IoT should be capable of interconnecting billions or trillions of heterogeneous objects through the internet, so there is a critical need for a flexible layered architecture.”*[1]

IoT Elements

> *"The heterogeneity of the IoT elements needs a thorough solution to make ubiquitous IoT services a reality."* [1]

To deliver complete functionality, the Internet of Things is broken into a multi-stage system that includes identification, sensing, communications, computations, services, and semantics. This interlinked network of information management and delivery supports the growing demands of the IoT, including data gathering, security, and delivery. At each stage, telecom organizations have opportunities to closely evaluate and innovate protocols and practices for maximum efficiency [1].

The Six Elements of IoT

There are six main elements needed to deliver the functionality of the IoT [1]:

Identification

Sensing

Computation

Communication

Services

Semantics

Identification

Identification methods provide a clear identity for each object within the network and match services with their demand from customers. Distinguishing between an object's identification and address is critical since identification methods are not globally unique. Numerous identification methods, such as ubiquitous codes (ucode) and electronic product codes (EPC), are available for the IoT [7].

Sensing and Control

IoT sensors can be smart sensors like wearable sensing devices, or actuators, which control such devices. These sensors gather data from related objects in a network and send it back to a data cloud, database, or warehouse. Next, the collected data is analyzed, and specific actions are taken based on services required.

Communication

Communication technologies of the IoT deliver specific smart services by connecting heterogeneous objects. These nodes frequently operate by using low power in the presence of lossy and noisy communication links [1].

Computation

TThe “brain” and the computational ability of the IoT include both hardware and software. Processing units include microcontrollers, microprocessors, SoCs, and FPGAs. These platforms rely on operating systems that run throughout the activation time of any device. [1, Tab. I] specifies several real-time operating systems (RTOS) best suited for the RTOS-based IoT applications [1].

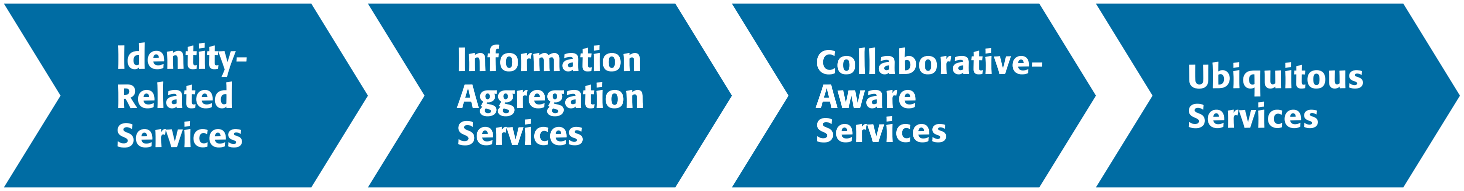
TABLE I. SPECIFICATIONS FOR REAL-TIME OPERATING SYSTEMS RECOMMENDED

Operating System	Language Support	Minimum Memory (KB)	Event-Based Programming	Multi-Threading	Dynamic Memory
TinyOS	nesC	1	Yes	Partial	Yes
Contiki	C	2	Yes	Yes	Yes
LiteOS	C	4	Yes	Yes	Yes
RIOT OS	C/C++	1.5	No	Yes	Yes
Android	Java	-	Yes	Yes	Yes

Services

As shown in [1, Fig. 4], services in the IoT are grouped into four categories:

- **Identity-Related Services** identify the real-world objects every application brings to the virtual world. As a result, they are the most basic and important and are used in the other classes of service.
- **Information Aggregation Services** collect and summarize raw sensory measurements that will be processed and reported to an IoT application.
- **Collaborative-Aware Services** act on top of Information Aggregation Services and use the resulting data to make decisions as well as formulate responses.
- **Ubiquitous Services** provide Collaborative-Aware Services *anytime* they are needed to *anyone* who needs them *anywhere*.


Identity-Related Services

Information Aggregation Services

Collaborative-Aware Services

Ubiquitous Services

Figure 4. IoT categories of services

The goal is to make all IoT applications ubiquitous.

Semantics

The semantic functionality ensures that the data extracted from the system is sent to the right resource. "Semantic," in the IoT, refers to the ability to extract knowledge smartly from different machines to provide the required services. Knowledge extraction includes discovering and using resources and modeling information. It also includes recognizing and analyzing data to make sense of the right decision to provide the exact service. Thus, semantics represent the brain of the IoT by sending demands to the right resource.

The six elements of IoT are reviewed in [1, Tab. II].

TABLE II. IoT ELEMENTS IN REVIEW

IoT Elements	Definition	Examples
Identification *Creates a clear identity for each object within the network and matches services with customer demand.*	**Naming:** Provides a clear identity for each object.	Electronic product codes (EPC) and ubiquitous codes (ucode)
	Addressing: Distinguishes between an object's identification and address. This is critical as identification methods are not globally unique.	IPv4, IPv6
Sensing and Control	Gathers data from related objects within the network and sends it back to a data warehouse, database, or cloud.	Smart sensors, wearable sensing devices, embedded sensors, actuators, RFID tags
Communication	Connects heterogeneous objects to deliver specific smart services.	RFID, NC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, Wi-Fi, Wi-Fi Direct, LTE-A

TABLE II. IoT ELEMENTS IN REVIEW (CONTINUED)

IoT Elements	Definition	Samples
Computation	**Hardware:** Includes processing units, such as microcontrollers, microprocessors, SoCs, FPGAs.	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, smartphones
	Software: Specifies essential operating systems that run for a device's whole activation time.	OS (Contiki, TinyOS, LiteOS, RIOT OS, Android); Cloud (Nimbits, Hadoop, etc.)
Services	Identity-Related (shipping)	Identify the real-world objects every application brings to the virtual world.
	Information Aggregation (smart grid)	Collect and summarize raw sensory measurements that need to be processed and reported to an IoT application.
	Collaborative-Aware (smart home)	Act on top of Information Aggregation Services and use the obtained data to make decisions and react accordingly.
	Ubiquitous (smart city)	Provide collaborative-aware services anytime they are needed to anyone who needs them, anywhere.
Semantics	Ensures that the data extracted from the system is sent to the right resource.	Resource Description Framework (RDF), Web Ontology Language (OWL)

IoT Standards

> *…[Protocol] standards help [the Internet of Things] to move one step forward towards enhancing the quality of life…”* [1]

Standards can be organized into four categories, which, although referenced in [1, Tab. III], do not have to be bundled together to deliver an application. From biometric open protocols to standards for local and metropolitan networks, IEEE offers standards on cutting-edge technologies shaping tomorrow's IoT-ready industries [1].

TABLE III. CATEGORIES OF IoT STANDARDS

Application Protocol		DDS	CoAP	AMQP	MQTT	MQTT-SN	XMPP	HTTP REST
Service Discovery		mDNS				DNS-SD		
Infrastructure Protocols	Routing Protocol	RPL						
	Network Layer	6LoWPAN				IPv4/IPv6		
	Link Layer	IEEE 802.15.4						
	Physical/ Device Layer	LTE-A	EPCglobal		IEEE 802.15.4		Z-Wave	
Influential Protocols		IPsec					IEEE 1905.1	

Additional IEEE Standards Related to IoT

IEEE has crafted thousands of standards for the connectivity that will shape the world of tomorrow. From healthcare to vehicles, these standards set the ground rules for future development of the Internet of Things.

IEEE Standard for Health Informatics PoC Medical Device Communication - Part 00101: Guide--Guidelines for the Use of RF Wireless Technology	IEEE 11073-00101™-2008
IEEE Standard Protocol for Stream Management in Media Client Devices	IEEE 2200™-2012
IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)	IEEE 1609.11™-2010
IEEE Standard for Air Interface for Broadband Wireless Access Systems Amendment: Enhancements to Support Machine-to-Machine Applications	IEEE 802.16p™-2012
IEEE Standard for Smart Transducer Interface for Sensors and Actuators Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats	IEEE 21451-7™-2011

Application Protocols

Extensible Messaging and Presence Protocol (XMPP)

A key element in telecom innovations is XMPP, a preferred protocol for most IM applications. It is an IETF instant messaging (IM) standard used for multi-party chatting, voice and video calling, and telepresence. Previously called Jabber, XMPP enables instant messaging over the internet regardless of individual operating systems [1].

> *"XMPP authenticates, controls access and delivers hop-by-hop and end-to-end encryption for IM applications."* [1]

Constrained Application Protocol (CoAP)

This web transfer protocol is based on representational state transfer (REST) on top of HTTP functionalities. REST simplifies the exchange of data between clients and servers over HTTP. Used within mobile and social network applications, the REST cacheable connection protocol relies on stateless client-server architecture. It also eliminates ambiguity by using HTTP GET, POST, PUT, and DELETE methods.

Message Queuing Telemetry Transport (MQTT)

This messaging protocol connects embedded devices and networks with applications and middleware. Defined specifically for sensor networks, MQTT offers routing mechanisms (one-to-one, one-to-many, many-to-many) that optimize connection protocols for the IoT and M2M. Its publish/subscribe pattern makes it easy to transition and implement, and it's suitable for resource-constrained devices that use unreliable or low bandwidth links [1].

Advanced Message Queuing Protocol (AMQP)

This open-standard application layer protocol focuses on message-oriented environments. It requires a reliable transport protocol like TCP to exchange messages. By defining a wire-level protocol, AMQP implementations can interoperate with each other.

Data Distribution Service (DDS)

This publish/subscribe protocol allows for real-time M2M communications. Unlike other protocols like MQTT or AMQP, DDS has a broker-less architecture and relies on multicasting. Thus, it offers excellent quality of service (QoS) and high reliability.

These application-layer protocols have attributes suiting them for specific scenarios and applications. As illustrated in [1, Tab. IV], there are a number of differences between the protocols that make it easy to choose one tailored to your application [1].

TABLE IV. COMPARISON OF APPLICATION PROTOCOLS

Application Protocol	RESTful	Transport	Publish/ Subscribe	Request/ Response	Security	QoS	Header Size (Byte)
CoAP	✓	UDP	✓	✓	DTLS	✓	4
MQTT	✗	TCP	✓	✗	SSL	✓	2
MQTT-SN	✗	TCP	✓	✗	SSL	✓	2
XMPP	✗	TCP	✓	✓	SSL	✗	—
AMQP	✗	TCP	✓	✗	SSL	✓	8
DDS	✗	UDP	✓	✗	SSL DTLS	✓	—

> “The **high scalability** of the IoT requires a resource management mechanism that is able to register and discover resources and services in a **self-configured, efficient, and dynamic way**.”[1]

Service Discovery Protocols

Service Discovery Protocols (SDP)

Service discovery protocols register and discover resources and services available through IoT devices. The dominant protocols are multicast DNS (mDNS) and DNS Service Discovery (DNS-SD). Although designed originally for resource-rich devices, these two protocols can be adapted for IoT environments.

Multicast DNS (mDNS)

For some IoT applications like chatting, mDNS can perform the task of a unicast DNS server. Because the DNS

> *"Although designed originally for resource-rich devices, light versions of MDNS and DNS-SD have been adapted for IoT environments."*[1]

space is used locally, mDNS offers flexibility without extra expenses or configuration [1].

The protocol is well-suited for embedded internet-based devices because:

- There's no need for manual reconfiguration or extra administration to manage devices
- It runs without infrastructure
- It continues to work if failure of infrastructure happens

DNS Service Discovery (DNS-SD)

DNS-based service discovery (DNS-SD) helps clients using mDNS find the services they're looking for. Using this protocol, clients can use standard DNS messages to discover the services they require in a specific network. DNS-SD, like mDNS, can connect machines without external administration or configuration [1].

Infrastructure Protocols

Routing Protocol for Low-Power and Lossy Networks (RPL)

RPL is a link-independent routing protocol based on IPv6 for resource-constrained nodes over lossy links. Built on a robust topology, the protocol supports simple and complex traffic models like multipoint-to-point, point-to-multipoint and point-to-point.

6LoWPAN

This protocol specifies the mapping services required by the IPv6 over Low-Power WPANs. It is an adaptation layer that fits IPv6 packets to IEEE 802.15.4 specifications. The standard provides header compression to reduce the transmission overhead, fragmentation to meet the IPv6 maximum transmission unit (MTU) requirement and forwarding to the link-layer to support multi-hop delivery [1].

IEEE 802.15.4

This protocol was created to specify a sublayer for Medium Access Control (MAC) and a physical layer (PHY) for low-rate wireless personal area networks (LR-WPAN) [1]. IEEE 802.15.4 can handle many nodes and provides reliable communication and operability on different platforms. The IoT, M2M technology, and wireless sensor networks (WSNs) opt for this protocol due to its low power consumption, low data rate, low cost, and high message throughput. While IEEE 802.15.4 provides a high level of security, encryption, and authentication services, it does not provide QoS guarantees.

Bluetooth Low Energy (BLE)

Also called Bluetooth Smart, BLE uses a short-range radio with a minimal amount of power to operate for a longer time. This efficiency makes it a good option for IoT applications compared to its previous versions. The range coverage of BLE is ten times that of classic Bluetooth technology with a range of about 100 meters and latency that is 15 times shorter. A transmission power between 0.01 to 10 mW can operate BLE [8]. Smartphone makers have rapidly developed the BLE standard, which is now available in most smartphone models.

EPCglobal

The Electronic Product Code (EPC) is a unique identification number stored on an RFID tag that is used to identify items in supply chain management. The underlying architecture relies on internet-based RFID technologies with RFID tags and readers to share product information. As well as supporting object IDs and service discovery, the openness, scalability, interoperability, and reliability of EPCglobal make it a promising technique for the future of the IoT [1].

Long Term Evolution-Advanced (LTE-A)

This set of cellular communication protocols is suitable for machine-type communications (MTC) and IoT infrastructures. It outperforms other cellular solutions in service cost and scalability. LTE-A is especially suitable to smart city applications, where long-term infrastructure durability is expected [9]. Recent advancements in LTE Category M and NarrowBand IoT (NB-IoT) technologies offer new options for longer battery life, improved speed, and quality in wireless communications.

Z-Wave

This low-power wireless communication protocol for home automation networks (HAN) is used extensively in smaller commercial domains as well as remote-control application in smart homes. Z-Wave covers about 30 meters point-to-point and is used for applications that require tiny data transmission. Such applications include light control, household appliance control, smart energy and HVAC, access control, wearable health care control, and fire detection. As shown in [1, Tab. V], each PHY protocol has various characteristics that work well for specific applications [1].

TABLE V. CHARACTERISTICS OF PHY PROTOCOLS

PHY Protocol	Spreading Technique	Radio Band (MHz)	MAC Access	Data Rate (bps)	Scalability
IEEE 802.15.4	DSSS	868/915/2400	TDMA, CSM/CA	20/40/250K	65K nodes
BLE	FHSS	2400	TDMA	1024K	5917 slaves
EPCglobal	DS-CDMA	860-960	Aloha	Varies 5-640K	—
LTE-A	Multiple CCs	Varies	OFDMA	1G (up), 500M (down)	—
Z-Wave	—	868/908/2400	CSMA/CA	40K	232 nodes

Other Influential Protocols

In addition to the standards and protocols that define an operational framework for IoT applications, there are some other considerations like security and interoperability that should be taken into account.

Security

Currently, security protocols on the internet operate over devices like desktop and laptop computers and are not suitable for the IoT. For comprehensive protection, new security protocols and architectures should be considered in all layers of the IoT, including securing data inside resource-constrained devices. As shown in [1, Tab. VI], there are not many security solutions at the application layer. Those available rely on security protocols at the transport layer i.e., either TLS or DTLS [1].

> ***"By 2022, M2M traffic flows will represent up to 45% of all internet traffic, requiring new security measures."[1]***

TABLE VI. APPLICATION-LAYER SECURITY PROTOCOLS

Layer	Application Level	Security Protocol	Solution
Application	File system	Codo (designed for Contiki OS)	Caches data for bulk encryption and decryption over wireless sensor networks (WSN)
Application	Link	IEEE 802.15.4	Protects communication between two neighboring devices on wireless personal area networks (WPANs)
Network		IPsec	Serves as mandatory security protocol for IPv6
Network		IPsec for 6LoWPAN	Serves application protocols that reply on TCP or UDP
Perception/ Transport		Transport Layer Security (TLS)	Secures TCP communications via cryptographic configuration
Perception/ Transport		Datagram TLS (DTLS)	Secures communications for diagram-based applications including UDP

Interoperability (IEEE 1905.1)

IEEE 1905.1 was designed as a standard for convergent digital home networks and heterogeneous technologies. Without requiring changes to underlying layers, IEEE 1905.1 provides an abstraction layer that hides the diversity of media access control (MAC) topologies. The protocol also delivers an interface to common home network technologies, allowing data link and physical layer protocols to coexist. Examples include IEEE 1901 over power lines, Wi-Fi/IEEE 802.11™ over the various RF bands, Ethernet over twisted pair or fiber cables, and MoCA 1.1 over coaxial cables.

While these standards help the IoT take another step toward enhancing quality of life, other concerns remain. These concerns include the environmental impact of IoT devices and technologies, as well as large scale and green deployment of IoT systems [1].

IoT Challenges and Future Directions

> *"The IoT, like other systems, needs to continuously develop and improve its services to meet customers' requirements."* [1]

As markets expand, demand for connected technology continues to grow. In 2016, Gartner predicted [5] 26 billion objects would be connected to the IoT by 2020, with an estimate by Cisco reaching 50 billion. Although forward-thinking telecom organizations recognize the power and potential of the IoT, many challenges remain in the way of a fully connected future. Cybersecurity presents a significant concern as the number of smart devices (and even cities) connected by the IoT continues to grow.

Recent reports in *IEEE Consumer Electronics Magazine* point to unsecured or poorly protected devices such as home security cameras, thermostats, and baby monitors, which can be hacked to reveal unencrypted personal data [5]. Providers in all markets, from smart homes to infrastructure, will look to telecom innovators to deliver protocols that combat data-mining [6] and other security breaches.

Along with security, other key issues to address include availability, reliability, mobility, performance, scalability, interoperability, management, and trust. Telecom service providers and application programmers who address these challenges will be able to efficiently implement their services.

Availability

The IoT must be available anywhere, anytime. Providing redundancy for critical devices and services will be one viable solution to achieve a high availability of IoT services.

Reliability

Reliability means guaranteeing the availability of information and services over time. This is even more critical when dealing with emergency response applications. In these critical systems, the communication network must be resilient.

Mobility

Applications and devices reliant on the IoT must continuously connect on-the-move users with their desired services while avoiding interruptions [1].

Performance

IoT service performance will only be as good as the individual components and underlying technologies. Many metrics will be used to assess the performance of the IoT, including processing speed, communication speed, device form factor, and cost.

Management

New protocols will be required to manage the fault, configuration, accounting, performance, and security (FCAPS) aspects of the billions or trillions of smart devices connected through the IoT.

Scalability

IoT applications must be designed from the ground up to enable extensible services and operations. This means the ability to add new devices, services, and functions must be built in without negatively affecting the quality of existing services [1].

Interoperability

Both application developers and IoT device manufacturers will have to build in end-to-end interoperability to ensure the delivery of services regardless of the specifications of the hardware platform that customers use.

Security and Privacy

Without a common standard and architecture for IoT security, it's not easy to guarantee users' security and privacy. The growing number of smart devices and applications using sensitive data necessitates transparent and easy-access control management. This approach will allow one vendor to read the data while another vendor controls the device. Proposed solutions include grouping embedded devices into virtual networks so only desired devices are presented within each virtual network. Access control can also be supported in the application layer on a per-vendor basis [1].

> “[There] is a need for an intelligent IoT gateway that offers ‘smart’ services that is deeply re-programmable through a rule-based language written by the programmer.”[1]

Preparing for a Connected Future

> *As scalability and interoperability have a great importance in IoT applications, augmenting the architecture with better abstractions can ease [architecture, scope, and infrastructure] issues.”* [1]

The rapidly expanding connectivity of the IoT is working to improve quality of life by integrating smart devices, technologies, and applications.

Businesses are also becoming rapid adopters of IoT technology, integrating new technology in connected factories that are able to optimize manufacturing efficiency with real-time data. The agriculture industry has begun to utilize farm equipment that can alert farmers to potentially catastrophic events immediately, potentially mitigating their devastating impacts.

These new technologies will still need to be aligned with business goals and show potential adopters that their investment will benefit the bottom line.

While the IoT will change every aspect of our daily lives, we shouldn’t overlook the very real challenges that will need to be addressed moving forward. Security and privacy will need to continue to be a top priority for IoT innovators. As IoT presses into new and uncharted territory, hackers will adapt and advance their methods to bypass the latest protections. The impacts from an unauthorized breach of data would be crippling for industries that handle sensitive information like health care and financial services.

Beyond privacy concerns, IoT devices continue to be a tool for DDoS attacks. And with continued exponential growth of IoT-enabled devices, the potential for DDoS attacks at unprecedented scales is significant.

Telecom networks that become targets of DDoS attacks and security breaches would begin to see trust in their networks and services erode. Ecommerce sites that suffer outages due to network downtime lose significant revenue and might be forced to find alternative solutions or close if those attacks aren't mitigated quickly. Data breaches have also resulted in significant financial settlements for companies involved. As the potential costs of a security incident increase, companies will become more actively involved in their network protection. Telecom companies and networks will need to show their customers that they are working to prevent the next attack, not just adapting to the last. That's why the development of industry-recognized security protocols and standards is so important.

Another pressing concern is energy usage. All IoT-enabled devices require energy, along with the wireless infrastructure required to support them. With the increase in connected devices, energy needs will be significant, as well as the energy required to power data centers to handle the exponential increase in traffic. [2]

The IoT's overall architecture, as well as its enabling technologies, protocols, and applications, continues to evolve. This ongoing evolution will provide new paths for telecom providers and developers to deliver specialized solutions that promise to revolutionize an industry.

IEEE *Xplore*® Digital Library

IEEE: The Leader in Telecommunications Research

This guide is brought to you courtesy of the IEEE *Xplore* digital library. To read the full article this white paper is based on, visit *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*. Additional articles, conference proceedings, standards, and research on the Internet of Things and other telecommunication technologies can be found in IEEE *Xplore*.

To see if your organization qualifies for a free trial of IEEE *Xplore*, visit:
ieee.org/telecom-free-trial

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Comm. Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[2] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, and L. Khoukhi, "IoT technologies for smart cities," *IET Networks*, vol. 7, no. 1, pp. 1–13, 1 2018.

[3] H. Almotiri, M. A. Khan and M. A. Alghamdi, "Mobile Health (m-Health) System in the Context of IoT," in *2016 IEEE 4th Int. Conf. on Future Internet of Things and Cloud Workshops (FiCloudW)*, Vienna, 2016, pp. 39–42.

[4] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in *2017 Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp. 477–480.

[5] P. Corcoran, "The Internet of Things: Why now, and what's next?," *IEEE Consum. Electron. Mag.*, vol. 5, no. 1, pp. 63–68, Jan. 2016.

[6] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[7] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things," *IEEE Pervasive Comput.*, vol. 9, no. 4, pp. 98–101, Oct.–Dec. 2010.

[8] J. DeCuir, "Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies," *IEEE Consum. Electron. Mag.*, vol. 3, no. 1, pp. 12–18, Jan. 2014.

[9] M. Hasan, E. Hossain, and D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 86–93, Jun. 2013.