ON OUR RADAR

Making IRL* Computable:

The Inevitable Internet of Things

by Ravi Pappu

* In Real Life

The Internet of Things (IoT) can be defined as the collection of physical objects that communicate their identity, state, and location to the internet. Much ink has been spilled about the number of things this collection might contain in 2020[1], the economic impact that the growth of IoT portends, and the benefit that IoT could have for our industries, cities, farms, vehicles, and even our bodies. However, those discussions offer little insight into how to think broadly about IoT systems, how these systems are put together, or how they might evolve. We consider these questions in this article. In service of clarity, we have omitted specific types of IoT sensors in this article, as that discussion does not necessarily enhance understanding of the bigger ideas at play.

What is IoT?

If you were to X-ray any of the numerous IoT systems in use today, you would see a skeleton that looks like Figure 1. Systems are comprised of *nodes*, which live in the physical world; *gateways* that enable the aggregation and forwarding of data from nodes; and the *internet*, where data is stored, analyzed, and made available for further consumption. This simple description belies the enormous complexity of these systems, but suffices to illuminate the dominant paradigm.

Before we explore the key ideas and the deeper structure of IoT systems, we present a quick look at IoT through the lens of prominent market verti-

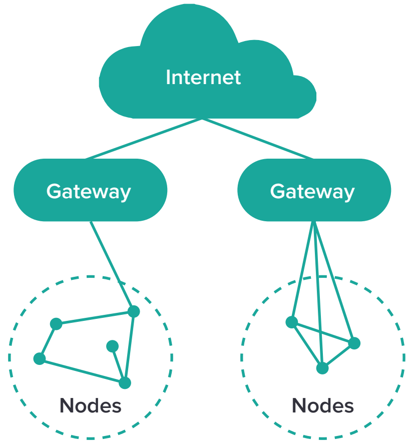


Figure 1 | The dominant paradigm of modern IoT systems, which comprise of nodes, gateways, and the internet.

cals. Our view is primarily informed by examples of what one can do with data collected from IoT nodes.

Market vertical	What is enabled or sensed?	What can be inferred?
Wearables	Physiological parameters, activity duration, location	State of health, psychographic information, patterns of life
Home	Presence, consumption of electricity, water, heat, presence of smoke, fire, carbon monoxide, particulate matter	Home activity, anomalies in consumption patterns, inventory levels
Telematics	Location, speed, bearing, vehicle parameters (fuel consumption, odometer reading, etc.), collisions	Wear and tear on vehicles, adherence to regulations, vehicle maintenance, anomalies in driving behavior, duration of and participation in congregative activities
Commerce	Items purchased and their location	Customer preferences, behavior, connections to payment accounts
Industrial IoT	Physical, chemical, and environmental parameters	Identity of objects, use of transportation systems, supply chain management, efficient use of resources, weather modeling
Robotics	Remote sensing and actuation, driverless cars	Elements of virtual presence, imagery, manufacturing statistics
Smart Cities	Traffic, utilities, waste management, fertilizer	Improved efficiencies, conservation, congestion control
Telemedicine	Physiological parameters, remote health, medication consumption	Population health and wellness parameters, disease prevalence and spread

As is evident from the table, running analytics on sensor data from IoT systems significantly broadens the range of inferences, and thereby, applications. Case in point: a $99 On-Board Diagnostics (OBD) peripheral for automobiles that contains a GPS sensor and can monitor vehicle Controller Area Network (CAN) bus data has enabled dozens of applications ranging from enhancing fuel efficiency to driver safety to expense reporting. It is important to note that the data (and metadata) were always there; the missing ingredients were the low-cost sensor and a means to communicate its data to the cloud. This is obvious, but worth remembering: *IoT makes invisible data visible.*

Fundamental Ideas

The current IoT revolution owes both its genesis and success to four fundamental ideas.

1) Software representations of physical things: Anything that can be represented by software will be represented by software. The first wave of software eating space and time was achieved by thinking deeply about separating the logical content of objects from their physical representation – cleaving the bits from the atoms. With bits in hand, atoms are dispensed with entirely, leading to a slow decline of things like *paper* books, *celluloid* film, and *metallic* coins. Today, even higher functions like operating a vehicle are representable as a combination of sensors and software. This drive toward higher levels of abstraction will no doubt continue relentlessly.

2) Invisible technology: As Marc Weiser so eloquently said, "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it[2]." Ubiquitous computing — the ability of computing, sensing, and communication technology to disappear into every object and enable those objects to be sensed by computers — has been pivotal in driving IoT forward.

3) Measurement, measurement, measurement: Software is eating the world, but the world can't eat software. Some of the largest challenges facing our species cannot be solved by code; we cannot program away climate change, water contamination, crowded cities, or hunger. However, measuring relevant quantities of interest can help model and understand these complex problems. To this end, IoT offers a scalable, effective, inexpensive, and persistent way of measuring a vast range of quantities.

4) Recombinant[3] technology capabilities: The more technology artifacts we have, the more we *will* have, owing to the power of recombination. Engineering relies on the encapsulation of discrete capabilities into modular artifacts that can then be combined to create new artifacts, which can themselves be modularized, and so on. Modern IoT is primarily based on synthesizing new applications by assembling existing technology capabilities in new ways and uniquely challenging their limits.

These four ideas make IoT inevitable. If we had not yet invented the idea of IoT, we would have to do so now. At this point, we are also in a position to define IoT succinctly: *the Internet of Things makes the real world amenable to computation.*

Six Core Capabilities of IoT Systems

IoT systems require six core technology capabilities, each of which is uniquely challenged by IoT applications. Innovation in any of these capabilities has the potential to significantly broaden the reach of IoT.

1) Communications: IoT needs radios that enable long-range communications at low data rates. It would not be an exaggeration to say that advances in low-cost and low-power radio communication have been pivotal in accelerating IoT deployments. While earlier generations of IoT systems were tethered to the internet with wires, the wireless communication revolution has had a direct causal impact on enabling, to paraphrase a cell phone commercial[4], more IoT in more places. The key requirements for IoT applications are:

- Long-range (miles, not feet) at low power consumption (milliwatts)
- Protocols optimized for short data payloads at low duty cycles as opposed to, for example, 4G-LTE, which is optimized for high bandwidths being utilized continually
- Support for mobility and in-building penetration
- A very low cost approaching $1 per module

In Figure 2 (opposite page), we take a look at the landscape for existing communication protocols as well as emerging protocols that are dedicated to IoT. As is clear from the figure, there are many incumbents[5] for short-range communication, but there is plenty of opportunity for long-range, low-bandwidth systems. This is the space that efforts like SigFox, Ingenu, LoRa, and the other Low-Power Wide Area Networking (LPWAN) efforts are targeting. However, cellular incumbents are developing flavors of LTE to bridge the gap from 4G to 5G, which promises support for IoT requirements from the get-go.

2) Hardware: IoT needs hardware that is low cost, low power, interoperable with a wide variety of sensors, and packaged in rapid prototyping kits to enable quick-turn application development.

Hardware is required to do several different things: general purpose computing, analog-to-digital conversion, storage, and communication. Node hardware spans many orders of magnitude in clock speed, cost, and capability – from a 7-cent passive RFID tag[6] to a portable weather station running on an 8- or 16-bit microcontroller at 20MHz. Node hardware has benefited tremendously from:

- **Moore's Law:** number of transistors per unit area doubles every 18 months
- **Koomey's Law:** number of instructions per joule grows more than Moore
- **Kryder's Law:** amount of storage per unit area also grows more than Moore

The convergence of scaling laws and the maker movement[7] has given rise to a large ecosystem of hardware for IoT applications in the form of single board computers such as Arduino, Raspberry Pi, Beaglebone, and Gumstick.

3) Software: IoT needs modular software that will run on different hardware architectures in resource-constrained environments (with low memory and clock speed). This

IQT Technology Architectures

A Technology Architecture is a unified, coherent structure that shows constituent technology capabilities and how those capabilities fit and work together.

In-Q-Tel's Technology Architecture Group is implementing a model on which Technology Architectures will be developed and used as a foundation for strategic investing against our customers' mission priorities. IQT's model for creating architectures is inspired by object-oriented design, which extends the principles of abstraction and re-use to define core technology capabilities.

By identifying capabilities and decomposing a system into individual core technology components, IQT is able to have more meaningful dialogue with customers. Technology conversations become easier and more contextual - we can discuss smaller components of the problem while keeping the holistic context of the problem intact. Legacy customer solutions and technologies can be mapped to the architecture in order to categorize and compare with potential solutions that exist in the commercial market.

software must be supported by a comprehensive menu of APIs, libraries, and wired/wireless networking stacks.

We are seeing these challenges addressed in two distinct ways: *top-down* and *bottom-up*. The top-down approach involves paring down existing operating systems like Linux and Android to fit the needs of IoT applications. For instance, Google's Brillo[7] is Android stripped down to run on constrained processors. However, these top-down efforts don't quite meet necessary resource constraints. The alternative bottom-up approach is essentially building an IoT operating system from scratch. There are a large number of such OSes available, the most prominent of which are Contiki, TinyOS, and Riot.

In addition, there are several industry alliances coalescing around different IoT verticals that aim to standardize interoperability between IoT devices. These projects, e.g., IoT@Work, Alljoyn, IPSO, and the Open Interconnect Consortium, are usually sponsored and led by large companies with current or future products in those verticals and are still in early stages of development.

4) Security: IoT needs security but it has often, and with very good reason, been called the Internet of Insecure Things[8] with "hilariously broken"[9] security. Nothing exemplifies this characterization more than a cursory browse through Shodan or Censys[10], search engines for IoT devices, which reveal vast numbers of devices without security controls. Some of these devices are innocuous, but many unsecured devices violate privacy or have the potential to cause severe disruption[11].

There are several reasons for this state of affairs. Building secure systems is challenging in any situation, and is exacerbated by the fact that IoT systems run in resource-constrained environments and are frequently deployed in remote locations by non-security professionals. The attack surface is simply too large.

In general, IoT security can be approached in two ways. The first is to optimize existing, well-understood cryptographic standards for operation on IoT nodes; the second, christened Lightweight Cryptography (LWC)[12], is to develop new cryptosystems for such devices. The security prescription for IoT devices can be stated quite simply: Use existing NIST standards wherever possible, because LWC is still in its infancy. We summarize the security landscape for IoT in Figure 3.

Fortunately, all of the major chipset vendors and IoT operating systems support NIST standards in their standard offerings. Some vendors are also offering trusted computing platforms like the Trusted Platform Module and Trusted Execution Environment in their products.

5) Management: With IoT, device management assumes outsized importance. There are three main reasons for this:

1) There are a multitude of nodes which are deployed in remote locations and only occasionally connected to the network;

2) The range and possibility of errors at the node are large; and

3) The cost of mismanagement (e.g., a botched over-the-air upgrade) is a "bricked"[13] node.

IoT device management can range from simple data collection to preemptive failure prediction with typical functions including initial device provisioning, firmware management, device monitoring, logging, and con-

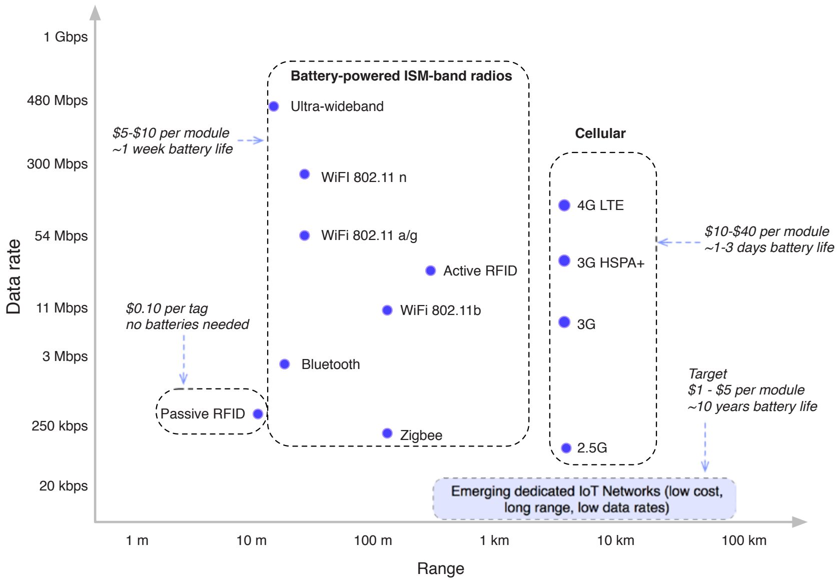


Figure 2 | This chart shows how IoT radios are dominated by short-range, high-bandwidth systems, while there is a need for long-range, low-bandwidth, and low-cost systems for many applications. These systems are depicted in the blue box in the figure. Note: this is not an exhaustive list of protocols and networks.

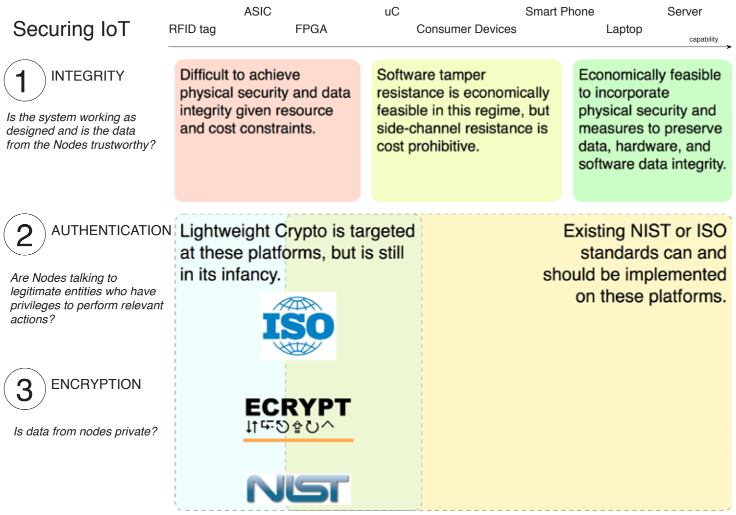

Securing IoT
ASIC
uC
Smart Phone
Server
RFID tag
FPGA
Consumer Devices
Laptop
capability
1 INTEGRITY
Is the system working as designed and is the data from the Nodes trustworthy?
Difficult to achieve physical security and data integrity given resource and cost constraints.
Software tamper resistance is economically feasible in this regime, but side-channel resistance is cost prohibitive.
Economically feasible to incorporate physical security and measures to preserve data, hardware, and software data integrity.
2 AUTHENTICATION
Are Nodes talking to legitimate entities who have privileges to perform relevant actions?
Lightweight Crypto is targeted at these platforms, but is still in its infancy.
Existing NIST or ISO standards can and should be implemented on these platforms.
3 ENCRYPTION
Is data from nodes private?
ISO
ECRYPT
NIST

Figure 3 | The state of IoT security. The axis at the top represents capabilities of IoT hardware. There are three main questions: Can we trust data from IoT nodes (integrity)? Are they talking to legitimate entities (authentication)? Is the data private (encryption)? For really constrained devices, trust is difficult to achieve, whereas for the medium and higher capability devices, it is technically feasible, but might not be economically feasible. With NIST standards, authentication and encryption are feasible in all but the lowest capability devices. Hence we prescribe using these existing standards wherever possible. Light Weight Crypto (LWC) is still in its infancy, but has several major contributors including NSA.

trolling nodes on demand (usually for troubleshooting purposes). We are seeing three approaches to IoT node management:

- Hardware vendors like ARM and Telit are including management capabilities as part of their product line. This includes software on the nodes to connect directly to their cloud platforms for management.
- Cloud computing incumbents like Amazon Web Services, Google Compute Engine, and Microsoft Azure are providing hardware-agnostic methods of getting IoT data into their cloud platforms.
- Hardware prototyping platforms like Arduino have management capabilities ported to run on them.

6. Analysis: IoT systems need analytics to aggregate noisy, granular data from the field and turn it into useful insight. This is what customers pay for.

In most IoT systems, analytics is where big data and data science collide. Many big data techniques are having a major impact on IoT data processing, including:

- New data abstractions for streaming data and distributed stream processing frameworks
- High-performance distributed data stores including NoSQL, time-series, in-memory, graphics processing unit (GPU), field-programmable gate array (FPGA), and geospatial databases
- Probabilistic algorithms
- Machine and deep learning
- Domain-specific analytic frameworks for applications including geospatial, transportation, agriculture, and mining

These core capabilities are visualized on page 10.

The Future of IoT

Predicting the future is hard, but it's clear that there is a fortune of economic and societal value at the bottom of the IoT pyramid[14]. As we said previously, some of humanity's hardest problems could leverage IoT to aid in understanding their scope and pointing the path towards solutions. Beyond the economic value and the number of devices, what can we expect to see as this IoT revolution unfolds? We conclude with one possibility.

Given the relentless drive towards software representations of everything, imagine that the cloud contains more and more sophisticated models, avatars, if you will, of all things IoT. Each of these models is occasionally in contact with its physical twin to refresh its state, but most of the commerce and transactions of data between these objects is happening predominantly in the cloud. What if these models include complete representations of farms, factories, vehicles, and cities? How might that change our economies, and, indeed, our world? Q

Dr. Ravi Pappu *is a Principal Architect in In-Q-Tel's Technology Architecture Group. Prior to joining IQT, Pappu held senior technology and management positions at Trimble Navigation and ThingMagic, a venture-backed company he co-founded. ThingMagic was acquired by Trimble in 2010. Pappu received his Ph.D. from the MIT Media Lab in 2001, and was named to Technology Review's TR100 list of top innovators under 35 and Boston Business Journal's 40 Under 40. He is no longer accepting any age-revealing awards.*

References

1. Estimates range from 21 to 50 Billion IoT devices by 2020
2. Weiser, Mark. The Computer for the 21st Century. Scientific American. September 1991.
3. Inspired by Recombinant DNA: DNA molecules formed by bringing together genetic material from multiple sources, creating sequences that would not otherwise be found in the genome.
4. Gardiner, Bryan. AT&T: 'More Bars in More Places' Is the New 'Fewest Dropped Calls'. Wired.com. http://www.wired.com/2007/08/att-more-bars
5. Morris, Iain. Vodafone to 'Crush' LoRa, Sigfox With NB-IoT. LightReading.com. http://www.lightreading.com/iot/vodafone-to-crush-lora-sigfox-with-nb-iot/d/d-id/722882
6. RFID Frequently Asked Questions. RFID Journal. https://www.rfidjournal.com/faq/show?85
7. Brillo. Google Developers. https://developers.google.com/brillo/
8. The Internet of Insecure Things. Forbes.com. http://www.forbes.com/sites/moorinsights/2015/09/.../the-internet-of-insecure-things/
9. Porup, J.M. "Internet of Things" security is hilariously broken and getting worse. Ars Technica. http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/
10. Shodan. https://www.shodan.io
11. Snow, John. What are IoT search engines Shodan and Censys and what are they capable of? Kaspersky Lab Official Blog. https://blog.kaspersky.com/shodan-censys/11430/
12. Lightweight Cryptography Workshop 2015. http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm
13. Bricked: To render completely useless, as useless as a brick.
14. Inspired by: Prahalad, C.K. and Stuart L. Hart. The Fortune at the Bottom of the Pyramid. http://www.stuartlhart.com/sites/stuartlhart.com/files/Prahalad_Hart_2001_SB.pdf

A Look Inside the Issue

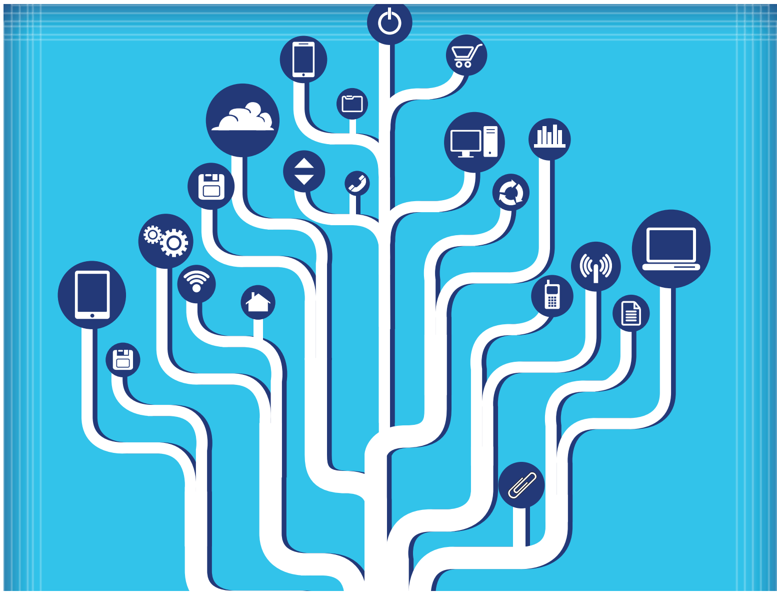
This issue of the *IQT Quarterly* examines the Internet of Things (IoT) revolution.

We begin with a Q&A with Kevin Ashton, a pioneer who is credited with coining the term "Internet of Things." He discusses the circumstances that led to his coining the now widespread term, and his experiences working on a global RFID standardization effort at MIT.

Peter Li discusses how Atlas Wearables is doing for human motion what Siri did for human voice, but without a tether to the cloud. The key ingredients of the Atlas recipe are low-cost, low-power 3D motion sensors and a learning system that runs on commodity microcontroller.

We then switch to the gateway layer of IoT. Peter Saint-Andre of Filament discusses a unique peer-to-peer, long-range radio communication system that uses smart contracts and private microtransactions to communicate and exchange value in a completely decentralized fashion.

Brad Keywell of Uptake then explains how to turn raw data from IoT sensors into knowledge by using modern big data technologies in the analytics layer. This layer is where domain-specific algorithms meet noisy, high-velocity data from the field.

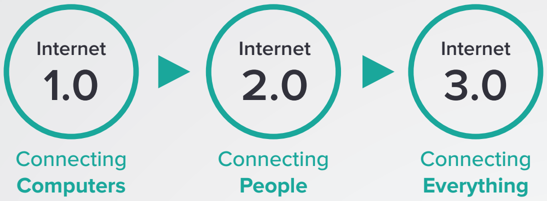


Finally, we look ahead to a crucial challenge that must be solved for IoT to expand its reach even further: energy. Josh Smith of the University of Washington presents the results of a decade of research that use the principles of passive RFID tags and show how they can be leveraged to harvest increasing amounts of energy from radio frequency transmissions. The devices range from an accelerometer to a microphone to a camera, all of which are powered solely by ambient RF. **Q**

The IoT Landscape

Internet 3.0: Connecting Everything

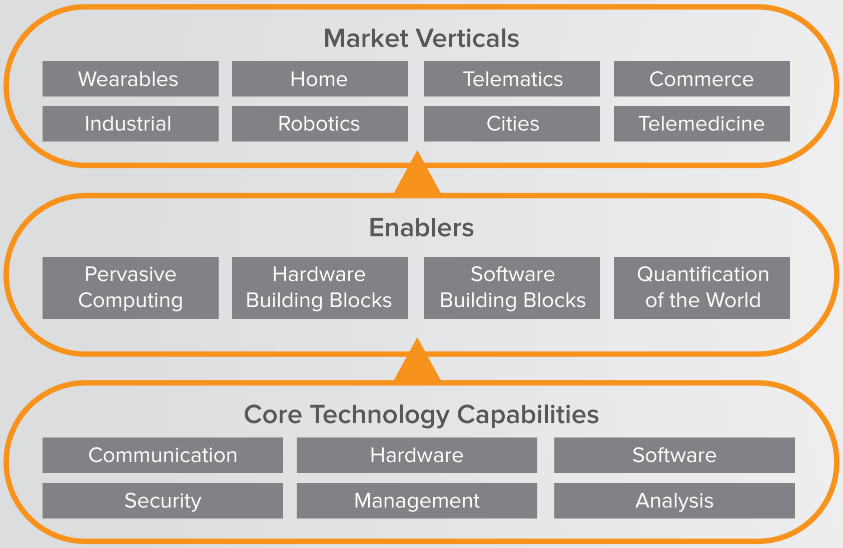
The internet (short for inter networking) was born of a need to connect computers to each other. This was followed by an explosion of applications, primarily connecting people to organizations and content and led to expansive growth in search, social networking, and commerce. The emerging IoT revolution promises to connect things in our physical world to the internet, dwarfing both the number of computers and the number of people on the internet by many orders of magnitude.



Internet 1.0
Connecting **Computers**

Internet 2.0
Connecting **People**

Internet 3.0
Connecting **Everything**



Market Verticals

Wearables, Home, Telematics, Commerce
Industrial, Robotics, Cities, Telemedicine

Enablers

Pervasive Computing, Hardware Building Blocks, Software Building Blocks, Quantification of the World

Core Technology Capabilities

Communication, Hardware, Software
Security, Management, Analysis

CONNECTED THINGS IN USE WORLDWIDE:

6.4B in 2016[1]

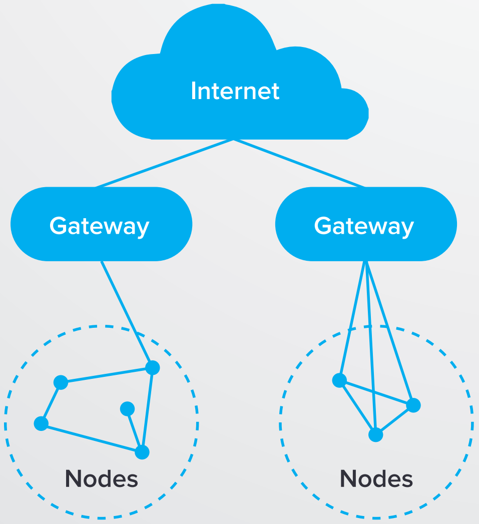
20.8B by 2020[1]

THE INTERNET OF INSECURE THINGS?

66% of networks will have an IoT security breach by 2018[2]

A Generic IoT System

The diagram to the right shows the dominant paradigm of modern IoT systems, which comprise of nodes, gateways, and the internet. Nodes can talk to each other and relay messages for other nodes via peer-to-peer communication, to an intermediary called the gateway via short-range communication, or directly to the internet via a cellular or satellite connection. There is a tremendous diversity of nodes owing to the broad range of IoT applications.



Enabling Technologies	Challenges	Advances
Communications	▪ Low cost ▪ Long range ▪ Low power ▪ Scalability ▪ Interoperability ▪ Efficiency ▪ Mobility	▪ IoT-specific communications protocols ▪ Optimization of existing cellular and short-range protocols
Software	▪ Constrained resources ▪ Scalability ▪ Modularity ▪ Connectivity ▪ Reliability	▪ IoT-specific operating systems (e.g., Contiki, TinyOS) support major multi-chip unit (MCU) families and networking protocols ▪ APIs for everything: sensor integration, device management, message brokering, and more
Hardware	▪ Size and compute power ▪ Battery life ▪ Adaptability ▪ Multi-sensor support	▪ Low-power memory ▪ Near and sub-threshold power ▪ Low-power communications
Security	▪ Usually absent ▪ Budget ▪ Constrained resources ▪ Remoteness ▪ Weak link ▪ Skills	▪ Optimizing NIST standards: reduction in Advanced Encryption Standard (AES) resource requirements, and Data Encryption Standard (DES) modifications ▪ Lightweight cryptography (LWC)
Management	▪ Constrained resources ▪ Scale ▪ Occasionally connected ▪ No downtime ▪ High penalty for failure	▪ Device services: registries, discovery, and search ▪ Purpose-built IoT platforms with APIs and SDKs that allow for node management ▪ Full stack development tools
Analysis	▪ Cost ▪ Range ▪ Power ▪ Scalability ▪ Interoperability ▪ Efficiency ▪ Mobility	▪ New streaming data abstractions ▪ Probabilistic algorithms ▪ High-performance distributed data stores ▪ Commoditization of machine and deep learning