Chapter 1
Internet of Things (IoT) Overview

The Internet of Things (IoT) has gained significant mindshare, let alone attention, in academia and the industry especially over the past few years. The reasons behind this interest are the potential capabilities that IoT promises to offer. On the personal level, it paints a picture of a future world where all the things in our ambient environment are connected to the Internet and seamlessly communicate with each other to operate intelligently. The ultimate goal is to enable objects around us to efficiently sense our surroundings, inexpensively communicate, and ultimately create a better environment for us: one where everyday objects act based on what we need and like without explicit instructions.

IoT's promise for business is more ambitious. It includes leveraging automatic sensing and prompt analysis of thousands of service or product-related parameters and then automatically taking action before a service experience or product operation is impacted. It also includes collecting and analyzing massive amounts of structured and unstructured data from various internal and external sources, such as social media, for the purpose of gaining competitive advantage by offering better services and improving business processes. This may seem like a bold statement, but consider the impact that the Internet has already had on education, communication, business, science, government, climate control, and humanity. Many believe that IoT will create the largest technology opportunity that we have ever seen.

The term "Internet of Things" was first coined by Kevin Ashton in a presentation that he made at Procter & Gamble in 1999. Linking the new idea of RFID (radio-frequency identification) in Procter & Gamble's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. He has mentioned, "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so." Afterward, the MIT Auto-ID center presented their IoT vision in 2001. Later, IoT was formally introduced by the International Telecommunication Union (ITU) *Internet Report* in 2005.

A. Rayes, S. Salam, *Internet of Things From Hype to Reality*,
https://doi.org/10.1007/978-3-319-99516-8_1

IoT is gaining momentum, especially in modern wireless telecommunications, as evidenced in the increasing presence around us of smart objects or things (e.g., smartphones, smart watches, smart home automation systems, etc.), which are able to communicate with each other and collaborate with other systems to achieve certain goals.

Undeniably, the main power of IoT is the high impact it is already starting to have on business and personal lives. Companies are already employing IoT to create new business models, improve business processes, and reduce costs and risks. Personal lives are improving with advanced health monitoring, enhanced learning, and improved security just to name few examples of possible applications.

1.1 What Is the Internet of Things (IoT)?

Before defining IoT, it may be worthwhile listing the most generic enablement components. In its simple form, IoT may be considered as a network of physical elements empowered by:

- *Sensors*: to collect information.
- *Identifiers*: to identify the source of data (e.g., sensors, devices).
- *Software*: to analyze data.
- *Internet connectivity*: to communicate and notify.

Putting it all together, *IoT is the network of things, with clear element identification, embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet*. IoT enables things or objects to exchange information with the manufacturer, operator, and/or other connected devices utilizing the telecommunications infrastructure of the Internet. It allows physical objects to be sensed (to provide specific information) and controlled remotely across the Internet, thereby creating opportunities for more direct integration between the physical world and computer-based systems and resulting in improved efficiency, accuracy, and economic benefit. Each thing is uniquely identifiable through its embedded computing system and is able to interoperate within the existing Internet infrastructure.

There is no disagreement between businesses and/or technical analysts that the number of things in IoT will be massive. Gartner says 20 Billion devices will be in used in 2020. Cisco estimate is 26.3 billion devices (including machine-to-machine devices, phones, TVs, PCs, tablets, and other connected devices) for the same period. Others believe this estimate to be overly conservative with the assumption that any object with a simple microcontroller, modest on-off switch, or even with QR (Quick Response) code[1] will be connected to the Internet in the near feature. Such a view is supported by Moore's Law, with the observation that the number of transistors in a dense integrated circuit approximately doubles every 18 months, as we will illustrate in Sect. 1.3.

[1] Quick Response Code is the trademark for a type of matrix barcode.

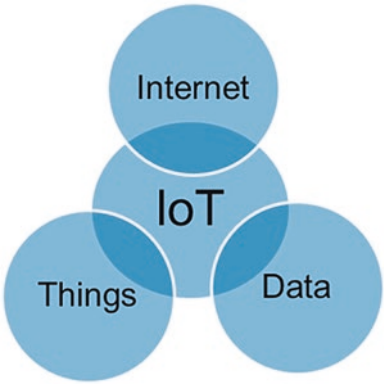


Fig. 1.1 IoT definition in its simplest form

The main idea of IoT is to physically connect anything/everything (e.g., sensors, devices, machines, people, animals, trees) and processes over the Internet for monitoring and/or control functionality. Connections are not limited to information sites, they're actual and physical connections allowing users to reach "things" and take control when needed. Hence, connecting objects together is not an objective by itself, but gathering intelligence from such objects to enrich products and services is.

1.1.1 Background and More Complete IoT Definition

Before we give historical overview of the Internet and consequently delve into the Internet of Things, it is worthwhile providing a definition and the fundamental requirements of IoT as a basis for the inexperienced reader.

We assume that the Internet is well known and bears no further definition. The question is what do we really mean by "Things[2]"? Well, things are actually "anything" and "everything" from appliances to buildings to cars to people to animals to trees to plants, etc. Hence, IoT in its simplest form may be considered as the intersection of the Internet, things, and data as shown in Fig. 1.1.

A more complete definition, we believe, should also include "Standards" and "Processes" allowing "Things" to be connected over the "Internet" to exchange "Data" using industry "Standards" that guarantee interoperability and enabling useful and mostly automated "Processes," as shown in Fig. 1.2.

[2] Some companies (e.g., Cisco) referred to IoT as the "The Internet of Everything." GE used the term "Industrial Internet" to refer to enterprise (nonresidential) Internet. Other companies have called it "The Internet of Anything." Other terms used for IoT include "Digital Disruptors," "The Nexus of Forces," and "The third Platform."

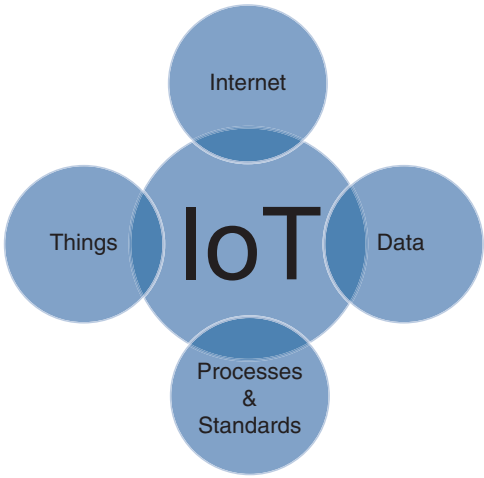


Fig. 1.2 IoT—more complete definition

Some companies (e.g., Cisco) refer to IoT as the IoE (Internet of Everything) with four key components: people, process, data, and Things. In this case, IoE connects:

- People: Connecting people in more relevant ways.
- Data: Converting data into intelligence to make better decisions.
- Process: Delivering the right information to the right person or machine at the right time.
- Things: Physical devices and objects connected to the Internet and each other for intelligent decision-making, often called IoT.

They correctly believe that today's Internet is the "Internet of People," i.e., today's Internet is mainly connecting applications that are used by people. People are taking action based on notifications from connected applications. IoT is envisioned to connect "things" where "things" (not people) will be taking action, when needed, by communicating with each other intelligently. IoE is then combining the Internet of People and the Internet of Things. In this book, and in most of the recent literature, however, IoT refers to anything and everything (including people).

With this in mind, we can state a more comprehensive definition of IoT as follows: *IoT is the network of things, with device identification, embedded intelligence, and sensing and acting capabilities, connecting people and things over the Internet.*

As we already mentioned above, we'll use the term "IoT" to refer to all objects/things/anything connected over the Internet including appliances, buildings, cars, people, animals, trees, plants, etc.

The basic promise of IoT is to monitor and control "things" from anywhere in the world. The first set of fundamental questions an engineer may ask are: How to monitor and control things from anywhere in the world? Why do we want to do so? Who will perform the monitoring and control? How is security guaranteed? In the remainder of this section, we will provide high-level answers to these questions. More detailed answers will be provided throughout the various chapters of this book.

1.1.2 How to Monitor and Control Things from Anywhere in the World?

Let's start with the first question. The basic requirements for IoT are the unique identity per "thing" (e.g., IP address), the ability to communicate between things (e.g., wireless communications), and the ability to sense specific information about the thing (sensors). With these three requirements, one should be able to monitor things from anywhere in the world. Another foundation requirement is a medium to communicate. Such requirement is typically handled by a telecommunications network. Figure 1.3 presents the very basic requirements of an IoT solution.

1.1.3 Why Do We Want to Monitor and Control Things?

There are many reasons to monitor and control things remotely over the Internet: monitoring and controlling things by experts (e.g., a patient's temperature or blood pressure while the patient is at the comfort of his or her own home); learning about things by pointing a smartphone to a thing of interest, for instance; searching for things that search engines (e.g., Google) do not provide today (e.g., where are my car keys); allowing authorities to manage things in smart cities in an optimal manner (e.g., energy, driver licenses, and other documents from Department Motor Vehicle,

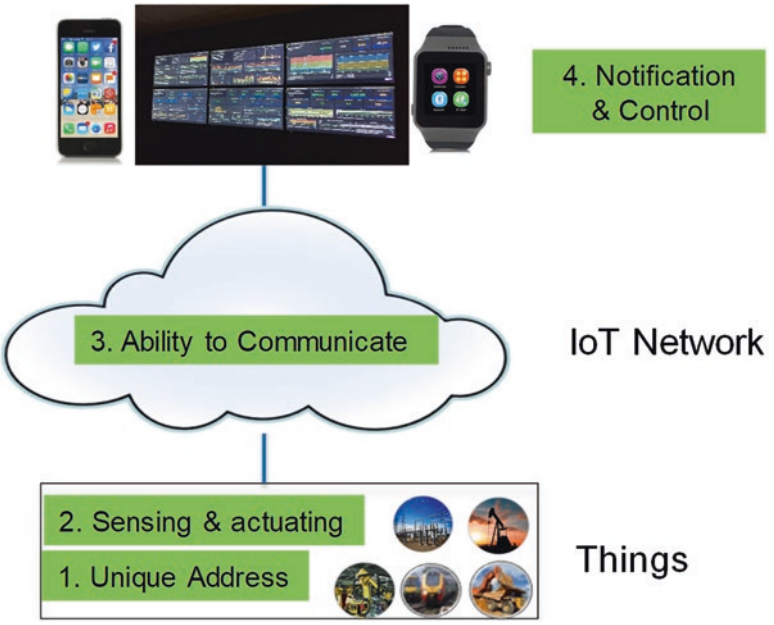


Fig. 1.3 Basic requirements for an IoT solution

senior citizen); and, finally, providing more affordable entertainment and games for children and adults. All of these are examples of huge business and service opportunities to boost the economic impact for consumers, businesses, governments, hospitals, and many other entities.

1.1.4 Who Will Monitor and Control?

Generally speaking, monitoring and control of IoT services may be done by any person or any machine. For example, a homeowner monitoring his own home on a mobile device based on a security system she or he has installed and configured. The homeowner may also control lights, turn on the air conditioning, shut off the heater, etc. Another example is for a service provider to monitor and control services for its customers in a network operations center (NOC) as shown in Fig. 1.4.

Obviously, security is a major concern to prevent access by non-authorized people and, more importantly, prevent a malicious hacker from gaining access to the system and sending old views to the homeowner while a thief is breaking in. The areas of control are far more critical for enterprise-sensitive applications such as healthcare monitoring of patients and banking applications, as we will see in Chap. 8.

Fig. 1.4 Example of monitoring systems in a network operations center

1.1.5 How Is Security Guaranteed?

Securing IoT is perhaps the biggest opportunity for technology companies and will remain so for some time in the future. Before IoT, information technology security professionals worked in a bubble as they literally owned and controlled their entire networks and secured all devices behind firewalls. With IoT, data will be collected from external, often mobile, sensors that are placed in public sites (e.g., city streets) allowing strangers to send harmful data to any network. Bring your own device (BYOD) is another example where third-party devices and hence noncorporate data sources are allowed to enter the network. IoT areas that are considered to be most vulnerable include:

- Accessing data during transport (network and transport security). Data will be transported in IoT networks at all time, for example, from sensors to gateways and from gateways to data centers in enterprises or from sensors to gateways for residential services such as video from home monitoring system to the home-owner's smartphone while he's in a coffee shop. This data may be sniffed by the man in the middle unless the transport protocols are fully secure and encrypted.
- Having control of IoT devices (control of the APIs) allows unauthorized persons to take full control of entire networks. Examples include shutting down cameras at home and shutting down patient monitoring systems.
- Having access to the IoT data itself. Is the data easily accessible? Is it stored encrypted? Shared storage in the cloud is another problem where customer a may log in as customer B and look at his data. Another common problem is spoofing data via Bluetooth. Many companies are adding Bluetooth support to their devices making it more feasible for unauthorized persons to access the device's data.
- Stealing official user or network identity (stealing user or network credentials). Many websites provide default passwords for vendors.

We have dedicated Chap. 8 to IoT security.

1.2 IoT Reference Framework

In this book, we will follow a reference framework that divides IoT solutions into four main levels: IoT devices (things), IoT network (infrastructure transporting the data), IoT Services Platform (software connecting the things with applications and providing overall management), and IoT applications (specialized business-based applications such as customer relation management (CRM), Accounting and Billing, and Business Intelligence (BI) applications). Control is passed down from one level to the one below, starting at the application level and proceeding to the IoT devices level and backup the hierarchy.

1. *IoT Device Level* includes all IoT sensors and actuators (i.e., the Things in IoT). The device layer will be covered in Chap. 3.
2. *IoT Network Level* includes all IoT network components including IoT gateways, routers, switches, etc. The (i.e., the Internet in IoT) will be covered in Chap. 2.
3. *IoT Application Services Platform Level* includes the key management software functions to enable the overall management of IoT devices and network. It also includes main functions connecting the device and network levels with the application layer. It will be covered in Chap. 7.
4. *IoT Application Level* includes all applications operating in the IoT network, and this will be covered in Chap. 9.

Figure 1.5 shows an overview of the IoT levels. It describes how information is transferred from one IoT component into another. Advantages of the proposed IoT four-level model include:

- Reduced Complexity: It breaks IoT elements and communication processes into smaller and simpler components, thereby helping IoT component development, design, and troubleshooting.
- Standardized Components and Interfaces: The model standardizes the specific components within each level (e.g., what are the key components for general IoT Services Platform) as well as the interfaces between the various levels. This would allow different vendors to develop joint solutions and common support models.
- Module Engineering: It allows various types of IoT hardware and software systems to communicate with each other.
- Interoperability between vendors by ensuring the various technology building blocks can interwork and interoperate.
- Accelerate Innovation: It allows developers to focus on solving the main problem at hand without worrying about basic functions that can be implemented once across different business verticals.

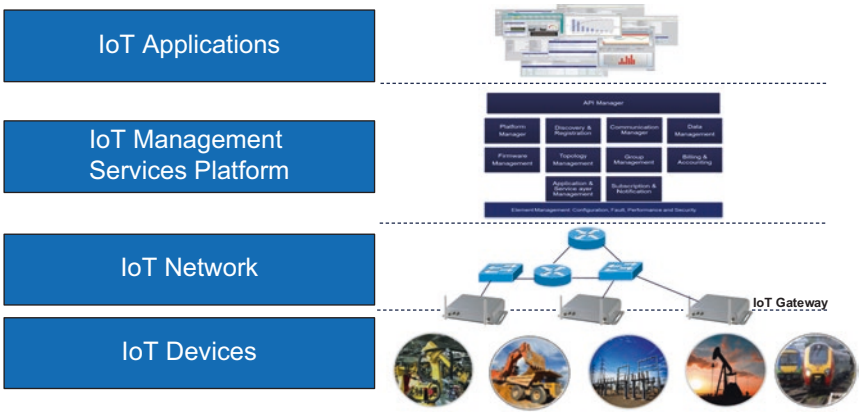


Fig. 1.5 IoT levels

- Simplified Education: It breaks down the overall complex IoT solution into smaller more manageable components to make learning easier.

1.3 Why Now? The 12 Factors for a Perfect Storm

IoT has already become a powerful force for business transformation, and its disruptive impact is already felt across all industries and all areas of society. There is a perfect storm of market disruptions happening at an unprecedented pace triggered by technology as well as new business and social requirements. This Section introduces the top 12 factors driving the explosion of IoT as shown in Fig. 1.6.

1.3.1 Convergence of IT and OT

Operation technology (OT) is the world of industrial plants and industrial control and automation equipment that include machines and systems to run the business, controllers, sensors, and actuators. Information technology (IT) is the world of end-to-end information systems focusing on compute, data storage, and networking to support business operation in some context such as business process automation systems, customer relation management (CRM) systems, supply chain management systems, logistics systems, and human resources systems.

Historically, IT and OT were always managed by two separate organizations with different cultures, philosophies, and set of technologies. IT departments were originally created by companies to create efficient and effective forms of telephony communication among various departments. Then they were extended to provide

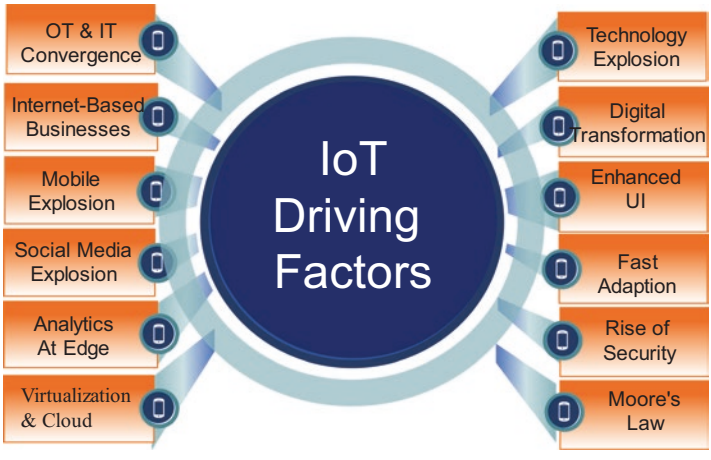


Fig. 1.6 IoT 12 driving factors

video and web conferences and network internal communications and secure external electronic communications such as emails. Often the final decision with the selection of communication systems, website hosting, and backup servers was the responsibility of the IT department.

OT relies on real-time data that drives safety, security, and control. It depends on very well-defined, tested, and trusted processes. Many plants need to run 24 × 7 with zero downtime (e.g., City Water Filtration System), and thus industrial processes cannot tolerate shutdown for software updates. IT is more lenient with software updates, introduction of new technologies, etc.

"When you take people with an IT background and bring them into an industrial control system environment, there's a lack of understanding from operations why they're there and there is a lack of understanding of the specific controls environment needs from IT," says Tim Conway, technical director, ICS and SCADA for the SANS Institute. He points out that typically IT professionals are trained and driven to perform a task: "They work on a box, a VM (virtual machine), a storage area network, or a firewall. They don't realize that they're a part of a larger control system operation, and how the things that they do can impact others."

IoT is having a major impact on OT and the traditional IT operational model. With the fast introduction of business-specific technologies (e.g., Internet-based oil rig monitoring systems), IT operations can no longer scale, keep up with the fast-evolving requirements, nor provide the required expertise. Traditional IT departments simply lack the required resources to introduce IoT solutions in a timely fashion, effectively operate and monitor such solutions, or react to the massive amount of monitoring data that is generated by IoT devices (Fig. 1.7).

The bottom line is that IT is moving fast into plant floors. With the pressure of IoT technology adoption by cutting-edge businesses, OT is forced to accept a greater

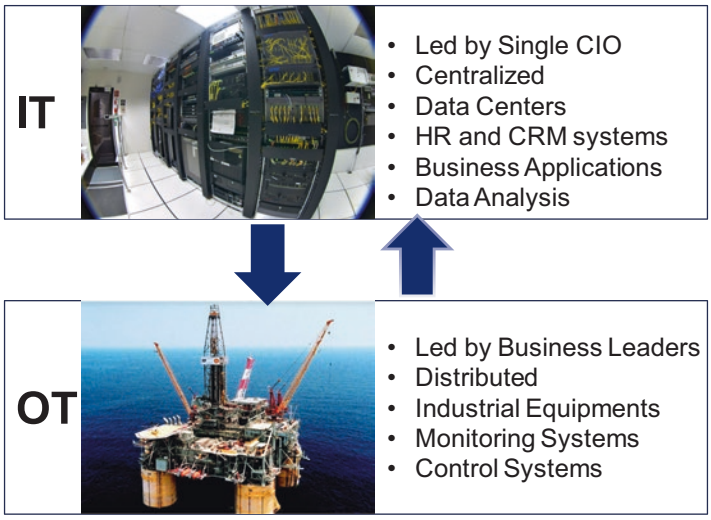


Fig. 1.7 The merger of IT and OT

level of integration. Hence, traditional IT and OT functions are expected to merge or quickly risk the loss of the business to cutting-edge competitors (why? See Problem 11). IT operations leaders must move closer to the business and adapt their employee skill sets, their processes, and their tools to monitor IoT availability and performance in order to support business initiatives as shown in Fig. 1.7.

1.3.2 The Astonishing Introduction of Creative Internet-Based Businesses

1.3.2.1 Uber

Many are familiar with Uber's story where the co-founders were attending a conference in Paris in 2008. Travis Kalanick and Garrett Camp were complaining about finding a cab especially while carrying luggage and under the rain. When they started to brainstorm the next day, they came up with three main requirements: the solution had to be Internet-based (i.e., request and track service from mobile device), it had to provide the service fast, and the rides had to be picked up from any location.

The key component of Uber's solution is the Internet-based platform connecting customers (passengers) with the service providers (car drivers). Because the consumers aren't Uber's employees and because there's practically an infinite number of cars that could potentially join Uber, Uber has the requirement to scale at an incredibly fast rate at zero marginal cost.

Uber uses sensor technologies in driver's smartphones to track their behaviors. If you ride with Uber and your driver speeds, breaks too hard, or takes you on a wildly lengthy route to your destination, it is no longer your word against theirs. Uber is using Gyrometer and GPS data to track the behavior of its drivers. Gyrometers in smartphones measure small movements, while GPS combined with accelerometers shows how often a vehicle starts and stops and the overall speed.

The idea is to gradually improve safety and customer satisfaction, though there's no word on whether or not you might be able to actively seek out a faster driver if that's what you're after.

Today Uber is one of the leading transportation services in the world with a market value over 20 billion dollars.

1.3.2.2 Airbnb

Airbnb is an Internet-based service for people to list, find, and rent lodging. It was founded in 2008 in San Francisco, California, by Brian Check and Joe Gebbia shortly after creating AirBed and Breakfast during a conference. The original site offered rooms, breakfast, and business networking opportunity for the conference attendees who were unable to find a hotel. In February 2008, technical architect Nathan Blecharczyk joined Airbnb as the third co-founder. Shortly thereafter, the

newly created company focused on high-profile events where alternative lodging was very limited.

Incredibly similar to the Uber model, Airbnb utilizes a platform business model. This means they facilitate the exchange between consumers (travelers) and service providers (homeowners). Airbnb also required a scalable Internet-based platform supporting from a few customers to hundreds of thousands during major events. More importantly, Airbnb is partnering with Internet companies (e.g., Nest of Google) to deliver remote keyless solutions to customers by unlocking doors (with IoT digital keys) over the Internet.

Just like Uber, Airbnb found a multibillion dollar business based on an Internet platform connecting people and places together that competently disrupted the traditional hotel business model. These linear businesses have to invest millions into building new hotels, while Airbnb doesn't have to deal with that.

Just like Uber, today Airbnb is one of the leading hotel services in the world with a market value close to 20 billion dollars.

1.3.2.3 Square

Square Inc., also San Francisco based, was inspired by Jack Dorsey in 2008 when his friend, Jim McKelvey, in St. Louis at the time, was unable to complete a $2000 sale of his glass faucets and fittings because he could not accept credit cards. Jack and Jim started the point-of-sale software financial services company in 2010. The company allows small business mobile individuals and merchants to make secure payments using applications like Square Capital and Square Payroll. The Internet-based software solution allows customers and small business owners to enter credit card information manually or to swipe the card via the Square Reader (see Fig. 1.9), a small plastic device that plugs into the audio jack of supported smart mobile devices with an interface resembling a traditional cash register.

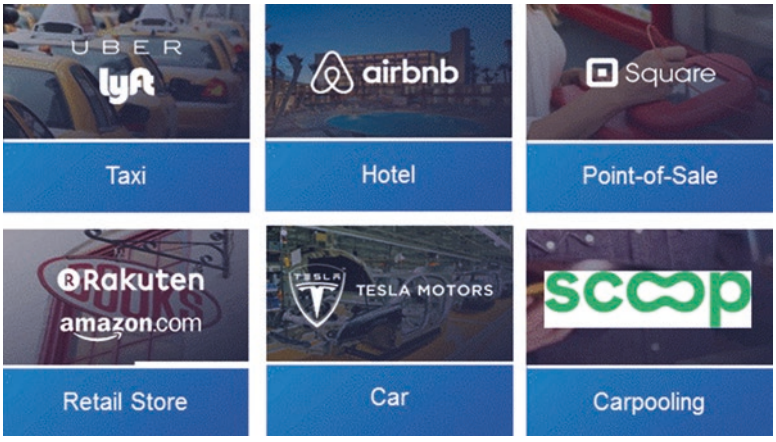


Fig. 1.8 Examples of Internet-based businesses

Square has introduced an application that integrates its reader with a smartphone's motion sensor. The application can determine that the card reader is failing by analyzing the motion sensor data to detect movements indicating multiple card swipes. If the card reader did not read any data during the card swipes, the application can deduce that the card reader is broken. This solution allows Square to send a replacement card reader to swap the broken card in a timely fashion.

Square also launched Square Cash applications allowing individuals and businesses to transfer money with a unique username. In 2015, Square introduced Customer Engagement, a suite of CRM tools which includes email marketing services. These tools allow businesses to target specific customer segments with customized promotions based on actual purchase history. Square also introduced Square Payroll tool for small business owners to process payroll for their employees.

Other financial companies have also introduced Internet-based mobile payment solutions including Intuit GoPayment Reader, which is integrated with Intuit's host of products and software (Fig. 1.10), PayPal Here Reader, and others.

Just like Uber and Airbnb, Square found a novel business based on Internet platform connecting small business owners and customers together that competently disrupted the traditional small business payment models.

Fig. 1.9 Square credit card reader. (Source: Square Inc.)

Fig. 1.10 Intuit GoPayment Reader. (Source: Intuit)

1.3.2.4 Amazon

Amazon.com is the largest Internet retailer company in the world with huge market cap over $300 billion dollars (as of late 2015). It started, in 1994, as an Internet-based book seller and swiftly expanded into music, movies, electronics, and household goods; Amazon utilized the Internet to break the traditional retailer model. It did not need to stock many of the merchandises it was selling on its website. Instead, it identified matching partner companies and issued customer orders over a secure Internet-based platform.

Amazon also offers businesses the capability to sell online via Amazon Services. Another part of its retail strategy is to serve as the channel for other retailers to sell their products and take a percentage of every purchase.

Retail is only part of Amazon.com business. It also offers cloud-based services known as Amazon Web Services or AWS with Software as a Services (SaaS), Platform as a Services (PaaS), and Infrastructure as a Services (IaaS) as well as other types of businesses such as Kindle. Amazon itself defines its lines of business in terms of product sales, service sales, cloud services, fulfillment, publishing, digital content subscriptions, advertising, and co-branded credit cards. Analysts have categorized Amazon's lines of businesses into online retail, Internet services, and the Kindle ecosystem. Based on April 28, 2016 reporting, AWS alone generated $8.9 billion in revenue between April 1, 2015, and March 31, 2016 (1 year).

Amazon is perhaps one of the first companies to develop a set of businesses based on an Internet platform connecting end customers (e.g., retail customer, businesses) to products and services (e.g., merchandise, cloud services) thereby disrupting traditional retail models.

1.3.2.5 Tesla

Tesla Motors was founded in 2003 by a group of engineers in Silicon Valley with a mission to develop a successful luxurious electrical car and then invest the resulting profits to make a less expensive electric car. With instant torque, incredible power, and zero emissions, Tesla's products would be cars without compromise.

Tesla's engineers first designed a power train for a sports car built around an AC induction motor, patented in 1888 by Nikola Tesla, the inventor who inspired the company's name. The resulting Tesla Roadster was launched in 2008 with an incredible range of 245 miles per charge of its lithium ion battery. The Roadster was able to set a new standard for electric mobility. In 2012, Tesla launched Model S, the world's first premium electric sedan.

Tesla is considered as the best example yet of IoT. It did not only bend the traditional industry manufacturing model to Internet-based model with thousands of sensors (Fig. 1.11), but it also demonstrated the tremendous value of IoT with the 2014 recalls. In early 2014, Traffic Safety Administration published two recall announcements, one for Tesla Motors and one for GM. Both were related to problems that

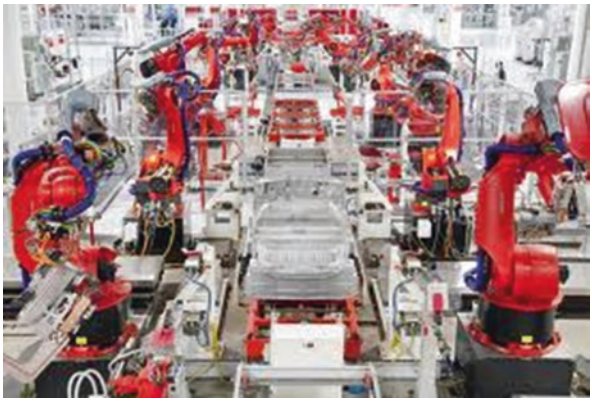


Fig. 1.11 Tesla Factory in Fremont, California. (Source: Tesla Motors Inc.)

could cause fires. Tesla's fix was conducted for 29,222 cars as an "over-the-air" software update without requiring owners to bring their cars to the dealer.

1.3.2.6 Self-Driving Cars

Self-driving cars are no longer a fantasy. There are already thousands of self-driving cars with features that allow them to brake, speed, and steer with limited or no driver interaction. Business Insider believes that 10 million self-driving cars will be on the road by the year 2020.

Self-driving cars can be divided into two main categories: semiautonomous and fully autonomous. A semiautonomous car performs certain self-driving tasks (e.g., fully brakes when it gets too close to an object, drives itself on the freeway), while a fully autonomous car drives itself from origin to destination without any driver interaction. Fully autonomous cars are further divided into user-operated and driverless. Because of regulatory and insurance questions, user-operated cars are expected to be available by 2018–2019 (pending regulatory and insurance issues), while driverless fully autonomous cars will be available at a later date.

Safety is considered one of the biggest advantages of self-driving cars. In the 6 years Google has had self-driving cars on the road with over 1.5 million miles, only 17 minor incidents have been reported, and none of those, prior to the February 2016 incident, were the self-driving car fault.

In general, self-driving cars are equipped with a large number of sensors including laser range finders (to measure a subject's distance and take photos that are in sharp focus), radars, and video cameras collecting information from the road. They're also equipped with actuators to control steering and braking. The collected data (from sensors, radars, and video) is promptly processed with the positional information from the car's GPS unit and the navigation system to determine its position and to build a three-dimensional model of its surroundings.

The resulting model is then processed by the car's control system to make navigation decisions. Self-driving car control systems typically use stored maps to find

Fig. 1.12 Google self-driving car. (Source: Google)

optimal path to destination, avoid obstacles, and send decisions to the car's actuators. IoT applies to interactions and communications between self-driving care components, between the car and roadside infrastructure, as well as among self-driving cars (Fig. 1.12).

Finally, it is worth noting that there are various other examples of companies that have used the Internet for new and creative business models, with various levels of success, including Scoop Inc. for carpooling and Pandora in the music industry.

1.3.3 Mobile Device Explosion.

There is an unprecedented explosion in the number of new things being connected to the Internet every day, where it isn't just sheer volume of mobile devices and sensors, but things that normally haven't been connected to the network, such as those found in manufacturing, utilities, and transportation, are all becoming networked devices. Because of the mobile explosion that has touched our home and work lives, we've already seen over 300,000 mobile applications developed in the past 3 years resulting in close to 11B downloads.

Mobile data traffic is expected to grow 18-fold in the next 5 years. According to Cisco's Visual Networking Index, smartphone traffic is set to grow from 1.74 exabyte per month in 2014 to more than 18 exabyte per months in 2019 as shown in Fig. 1.10. Cisco further estimates that smartphones will account for 75% of mobile traffic in 2019, up from 69% in the past year.

The increase in mobile data traffic is driven by two factors: the increase in the number of users and the data consumption per user. The average smartphone will expectedly generate 4 GB of traffic per month in 2019, a fivefold increase over last year's global average. This growth will definitely be fueled by IoT connecting things

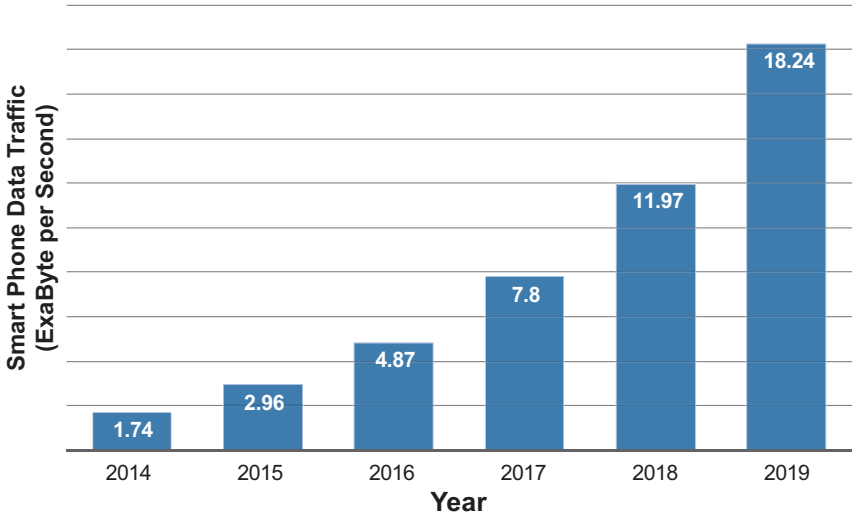


Fig. 1.13 Smartphone traffic over time

with people and more importantly allowing people to monitor and control things from anywhere in the world in real time. Figure 1.13 shows smartphone traffic growth (in exabyte per second) between 2014 and 2019 based on data published by Statista.

1.3.4 Social Network Explosion

Social networks, such as Facebook, Instagram, Twitter, and YouTube, and the adoption of cloud-based services, such as Amazon's AWS and Salesforce.com, are all examples of the large-scale migration to the cloud across virtually every industry. In fact, two thirds of all data center traffic will be from the cloud in 3 years. All of this leads to data explosion, where, already, the data being created on the Internet each day is equal to half of all the data that has been accumulated since the dawn of humanity (Fig. 1.14).

1.3.5 Analytics at the Edge

Before introducing the different versions of analytics, it's important to define the terms: big data, structured data, and unstructured data. Big data refers to the extremely large amount of data being generated and accumulated by IT systems as the result of the operation of an associated system. The latter could be a product,

Fig. 1.14 Examples of social network explosion

process, service, etc. This massive amount of data can be analyzed to identify patterns and gain insights into the operation of the associated system. The analysis often involves applying statistical techniques since human processing is not viable due to the sheer volume of the data.

Structured data refers to organized data that can fit in rows and columns. Examples of such data include customer data, sales data, and stock records. Structured data is often high value, cleansed, and indexed. Unstructured data, on the other hand, is difficult to organize or bring together. Examples of unstructured data include images, X-rays, video, social media data, and some machine outputs mixed with text.

Analytics 1.0 refers to the process of collecting structured data from various sources and sending the collected data to a *centralized* location to be correlated and analyzed using predefined queries and descriptive/historic views. Businesses and enterprises have been collecting structured data from internal systems (e.g., CRM, Sale Records, RMA Records, and Case Records), sending such data to a centralized data center to be stored in traditional tables and databases. The data is then parsed and often correlated with other types of data to produce business intelligence (e.g., offer discounts for customers in a certain location due to large unused inventory). The process of collecting, transferring, correlating, and analyzing the structured data can take hours or days.

Analytics 1.0 then evolved to Analytics 2.0 or big data and analytics with actionable insight. Analytics 2.0 basically collects structured and unstructured data from various sources but still sends the collected data to a *centralized* location to be correlated and analyzed using complex queries along with forward-looking and predicative views this time. Examples of unstructured data for enterprises include call center logs, mobility data, and social media data where users are conversing and providing feedback about an enterprise's service, product, or solutions.

Table 1.1 Comparison of key factors for Analytics 1.0, 2.0, and 3.0

	Analytics 1.0	Analytics 2.0	Analytics 3.0
Collected data type	Structured	Structured and unstructured	Structured and unstructured
Data analysis location	Centralized data center	Centralized data center	At edge and in data center
Time to analyze data	Days–hours	Hours–minutes	Seconds–microseconds
Data volume	Small data	Big data	Big data

With the deployment of complex systems to capture and analyze big data in a datacenter, the overall process of collecting, transferring, correlating, and analyzing the structured and structured data is reduced to minutes or seconds.

Today, massive amounts of data are being created at the edge of the network, and the traditional ways of performing analytics over that data are no longer viable. Minutes or even seconds of delay in data processing are no longer effective for many businesses. Take, for example, a sensor in an oil rig. If the pressure were to drop substantially, the rig needs to be shut off instantaneously and before the system breaks and causes a major disaster.

Companies are realizing that they just cannot keep moving massive amounts of data to centralized data stores. The data is too big, is changing too fast, and is too geographically distributed. Certain analysis must be performed in real time and cannot withstand the delays of sending the raw data to a centralized data center to be analyzed and then send back the result to the source. In addition, certain industries (e.g., Healthcare, Defense) have the requirement to analyze the data close to the source due to data privacy or security.

Analytics 3.0 allows companies to collect, parse, analyze, and correlate (with stored data) structured as well as unstructured data at or close to the edge (the source of the data). To support this, companies have introduced massive solutions (hardware and software) that allow enterprises to capture, process, and analyze data at the edge. Can you think of examples of such companies (see problem 15)?

Analytics 1.0, 2.0, and 3.0 are compared in Table 1.1 and in Fig. 1.15: Table 1.1 shows a comparisons of key factors, while Fig. 1.15 displays a process summary.

1.3.6 Cloud Computing and Virtualization

Up until recently, enterprises (companies or businesses) were forced to deploy and manage their own computing infrastructures. Cloud computing, which was introduced in 2008, allows enterprises to outsource their computing infrastructure fully or partially to public cloud provides (e.g., Amazon AWS, Microsoft Azure, Google Compute Engine). Recent data showed that the average network computing and storage infrastructure for a start-up in year 2000 was $5 million. The cost in year

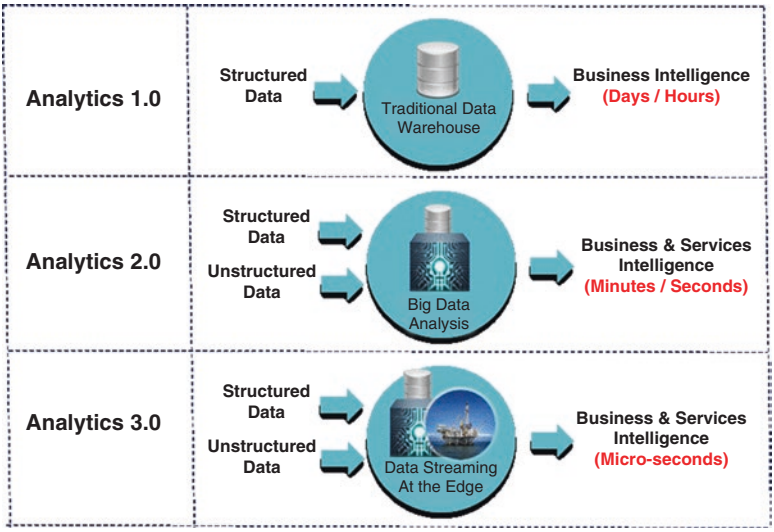


Fig. 1.15 Analytics 1.0, 2.0, and 3.0

2016 has dropped to $5 thousand. This enormous 99% decline in cost was made possible by cloud computing and vitalization.

Public Cloud providers deliver cloud services, on demand, over the Internet. Enterprises pay only for the CPU cycles, storage, or bandwidth they consume.

Enterprises also have the choice to deploy *Private Cloud* solutions in their own data centers and deliver computing services to their internal sub-businesses/users. Such model offers flexibility and convenience while preserving management, control, and security to their IT departments.

Cloud computing may be also offered in a *Hybrid Cloud* model that consists of a combination of public and private clouds allowing enterprises to create a scalable solution by utilizing the public cloud infrastructure while still preserving full control over critical data.

Cloud computing is attractive to many enterprises allowing them to self-provision their own services for any type of workload on demand. They can start small and then scale up almost instantly with minimum expertise and pre-planning, while they pay only for what they use, typically, in addition to a basic subscription charge.

Cloud computing has been classified into three main service categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as Service (SaaS). PaaS, for instance, allows enterprises to utilize a third-party platform and permits them to focus on developing and managing their own software applications without the complexity of building and maintaining the required infrastructure.

Cloud computing has been made possible by the advent of *virtualization* technologies. Rather than dedicating distinct IT infrastructure (e.g., servers, storage nodes, networking nodes) to a single business entity (e.g., customer or enterprise),

virtualization allows cloud providers to divide a physical machine (e.g., server) into multiple virtual entities thereby creating an isolated virtual server, a virtual storage device, and virtual network resources for each enterprise, all running over the same shared physical IT infrastructure. Virtual machines are one form of virtualization that allows running multiple operating systems over the same physical server hardware.

Containers are another form of virtualization. In containers, the virtualization layer runs as a service on top of a common operating system kernel. The operating system's kernel runs on the hardware node with several isolated guest process groups installed on top of it. The isolated guest process groups are called containers. They share the same operating system kernel but are completely isolated at the application level.

Containers are intended to run separate applications. Examples of containers include Linux containers (LXC) and open-source Docker.

As with Analytics (Sect. 1.3.5), Cloud may be divided into Cloud 1.0 and Cloud 2.0. Cloud 1.0 is SaaS, PaaS, and IaaS. Cloud 2.0 is Cloud 1.0 with machine learning to extract business intelligence from the data using algorithms that learn from data pattern. It should be noted that traditional techniques and machine learning programs work without specific instructions on where to look for data pattern.

1.3.7 Technology Explosion

IoT hardware (e.g., sensors, inexpensive computers such as Raspberry Pi, open source microcontrollers such as Arduino) and software technologies are not only being developed faster than ever before but with much lower prices. Such devices are already transforming user behaviors and creating new business opportunities. Business leaders are realizing that unless their organizations quickly adapt to such changes, their businesses will soon become irrelevant or inefficient to survive in an increasingly competitive marketplace.

1.3.8 Digital Convergence/Transformation

Digital convergence has initially started with a limited scope: move to "paperless" operation, and save trees. Now, it is transforming the future in profound ways. Digital convergence is being adopted by key industries with extended goals to move to digital operation, extract data from various sources including the devices and processes that are enabled by digitization, and then analyze the extracted data and correlate it with other data sources to extract intelligence that improves products, customer experience, security, sales, etc. Many healthcare organizations (e.g., Kaiser Permanente) have been using digital convergence with extended goals of improving the patient experience, improving population health, and reducing healthcare costs.

With the connection of 50 billion smart objects to the Internet by 2020, companies are realizing the upcoming challenges and are adding to their executive boards the role of a Chief Digital Officer (CDO) who can oversee the full range of digital strategies and drive change across the organization. CDOs are expected to significantly impact existing systems, solutions, and business processes and more importantly intrinsically enable new types of innovation and creativity.

1.3.9 Enhanced User Interfaces

User experience (UX) or human to machine interaction, where applicable, is very essential for the success of IoT. A core IoT UX principle is meeting the basic needs for the usage of a product or a service without aggravation or difficulty. Overengineering or including too much intelligence into products can backfire and be counterproductive. User interfaces that are frustrating to use and slow to extract relevant information can lead to customer desertion. A toaster, for example, ultimately exists to make toast. But if we overengineer with too much information, switches, and options, we risk building products that are so annoying that our customers won't want to use them.

There is now a wealth of technology and markup languages (e.g., HTML 5) that allow software engineers to adapt key UX principles and meet the so-called KISS (keep it short and simple) principle. KISS states that most systems work best if they are kept simple. Top UX principles include:

- *Simple and Easy Principle:* Best UX system is a system without UI. Simplicity should be a key goal in design, and unnecessary complexity should be avoided. Make sure you reduce the user's cognitive workload whenever possible. Make sure the UI is consistent/stable, intuitive, and establish a clear visual hierarchy.
- *Contextual Principle:* Make sure that users are contextually aware of where they are within a system.
- *Human Principle:* Make sure the UI provides human interactions above the machine-like interactions.
- *Engagement Principle:* Make sure that the UI fully engages the user, delivers value, and provides a strong information sense.
- *Beauty and Delight Principle:* Make sure the UX is enjoyable and make the user wants to use the system or service.

1.3.10 Fast Rate of IoT Technology Adoption (Five Times More than Electricity and Telephony)

Many of us are changing our mobile devices and tablets at faster rate than ever before. Experts believe that there was a point of inflexion sometime between 2009 and 2010, where the number of connected devices began outnumbering the planet's

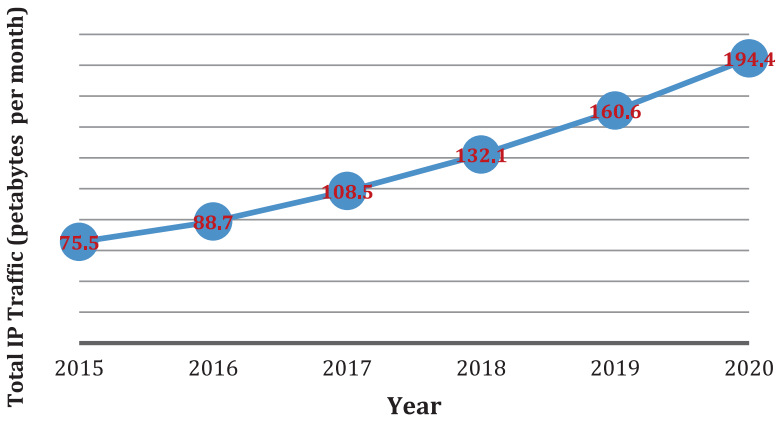


Fig. 1.16 Global IP traffic growth, 2015–2020. (Source: 2016 Cisco VIN)

human population. And these aren't just laptops, mobile phones, and tablets—they also include sensors and everyday objects that were previously unconnected. Surveys and detailed analysis indicated that the adoption rate of such technology is five times faster than that of electricity and telephony growth. Traditionally the adoption of technology was always proportional to population growth. Hence, IoT adoption gap is expected to widen exponentially over the next several years, with the number of sensors, objects, and other "things." This is best illustrated by global IP traffic growth, as shown in Fig. 1.16. According to June 2016 Cisco Visual Networking Index (VNI) forecast, global IP traffic in 2015 stands at 72.5 exabytes (EB, 10^{18} byte) per month and will nearly triple by 2020, to reach 194.4 EB per month. Consumer IP traffic will reach 162.2 EB per month, and business IP traffic will surpass 32.2 EB per month by 2020.

Adding all of these physical objects to IP networks imposes new and novel requirements on existing networking models. ITC will need to deal with those requirements in a relatively short order.

1.3.11 The Rise of Security Requirements

Protection of business and personal data and systems has been an issue since the inception of data networks. With the commercialization of the Internet, security concerns expanded to cover personal privacy, financial transactions, and the threat of cyber robbery. Today, security of the network is being expanded to include safety or physical security.

Many of us are buying and deploying smart gadgets all over our homes. Examples include smart cameras that notify our smartphones during business hours when movement is detected, smart doors that open remotely, and the smart fridges that notify us when we are short of milk. Imagine now the level of control that an attacker can gain by hacking those smart gadgets if the security of those devices were to be

overlooked. In fact, the damage caused by cyber-attacks in the IoT era will have a direct impact on all the physical objects that you use in your daily life. The same applies to smart cars as the number of integrated sensors continues to grow rapidly and as the wireless control capabilities increase significantly over time, giving an attacker who hacks a car the ability to control the windshield wipers, the radio, the door lock, and even the brakes and the steering wheel of the vehicle. Our bodies won't also be safe from cyber-attacks. In fact, researchers have shown that an attacker can control remotely implantable and wearable health devices (e.g., insulin pumps and heart pacemakers) by hacking the communication link that connects them to the control and monitoring system.

1.3.12 The Nonstop Moore's Law

It is possible to summarize Moore's Law impact with three key observations:

1. Over the history of computing hardware, computer power has been doubling approximately every 18 months. This relates to the fact that the number of transistors in a dense integrated circuit has been growing by twofold every 18 months since the transistor was invented in 1947 by John Bardeen, Walter Brattain, and William Shockley in Bell Labs, as shown in Fig. 1.17.

   Now, the largest existing networks in 2016 contain millions of nodes and billions of connections. Human brains, on the other hand, are about a hundred thousand times more powerful. A human brain has one hundred thousand billion nodes and a hundred trillion connections. Hence, with Moore's Law, a computer should be as powerful as the human brain in about 25 years!
2. Silicon transistor storage technology size has continued to shrink over the years and is approaching atomic level. For years now, we've been putting more power and more storage on the same size device. To illustrate this idea, the number of all transistors in all PCs in 1995, a peak year for Microsoft, was about 800 trillion transistors. Today, 800 trillion transistors are included in one weekend's sales of Apple's iPhones.
3. The price of the transistor is being reduced by more than 50% every year. In 1958 Fairchild Semiconductor procured its first order for 100 transistors at $150 apiece from IBM's Federal Systems Division. Today, you can buy over one million transistors for 8 cents. Figure 1.17 shows such trend over time.

There is no exact number for the estimated IoT revenue for the next 10 years, but all industry leaders have agreed that the opportunity is indeed huge.

A study by General Electric, which likened the IoT trend to the industrial revolution of the eighteenth and nineteenth centuries, concluded that the IoT over the next 20 years could add as much as US $15 trillion to the global gross domestic product (GDP)—which is roughly the size of today's US economy.

As we mentioned before, Cisco believes there will be 32 billion devices connected to the Internet by 2020. That translates to four devices for every person of the

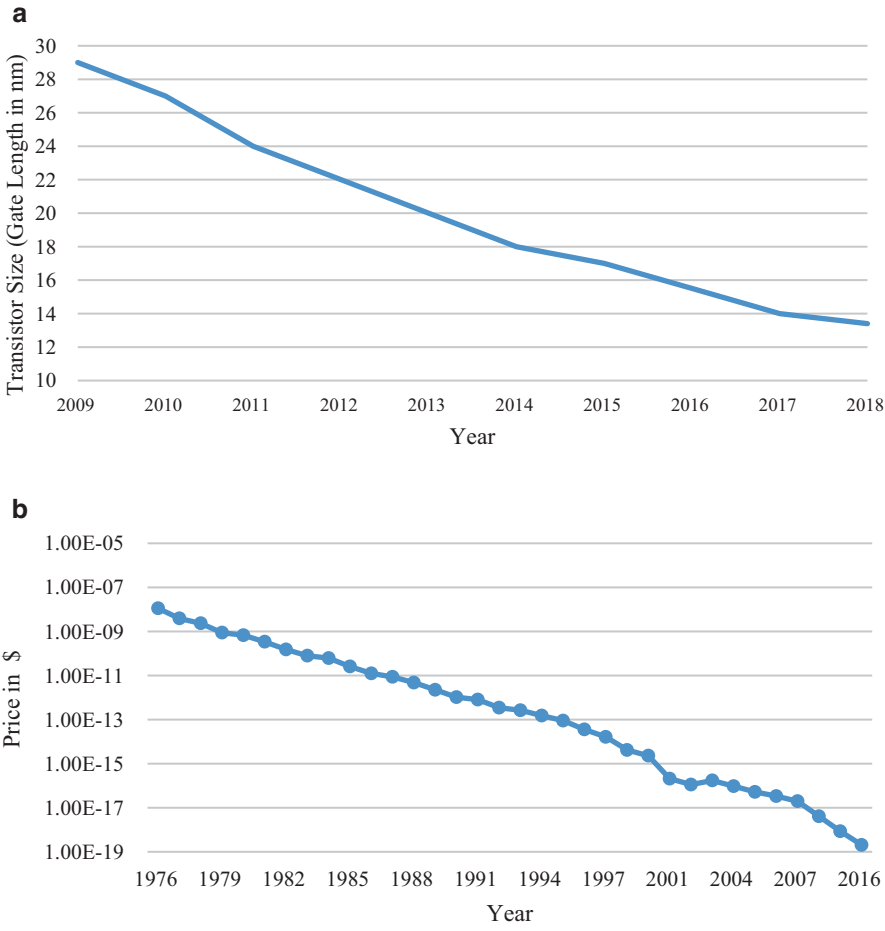


Fig. 1.17 Moore's Law: (**a**) transistor size over time, (**b**) transistor price over time

8 billion people that are expected to be around in a few years. To help put that in more perspective, Cisco also came out with the estimate of 8.7 billion devices that were connected to the Internet in 2012. These devices mainly comprise of the PCs, laptops, tablets, and phones in the world. But other types of devices will soon dominate the collection of the Internet of Things, such as sensors and actuators. Counting the number of miniscule chips, Intel and IDC believe that the number of IoT devices will reach 200 billion in 2020.

By the end of the decade, a nearly ninefold increase in the volume of devices on the Internet of Things will mean that significant infrastructure investment and market opportunities will exist in this sector. Cisco believes that it will translate to a $14-trillion industry. This includes $2.5T in asset utilization, $2.5T in employees' productivity, $2.7T in supply chain logistics, $3.7T in customer expenditure, and $3T in innovations.

Table 1.2 IoT units installed base by category, excluding automotive

Category	2014	2015	2016	2020
Consumer	2277	3023	4024	13,509
Generic business	623	815	1092	4408
Vertical business	898	1065	1276	2880
Grand Total	**3807**	**4902**	**6392**	**20,797**

Source—Gartner, 2015

Gartner, Inc. has published the number of "things" connected over the Internet as shown in Table 1.2. Without automotive, the total number of expected IoT installed-based devices is estimated to be close to 21 billion in 2020. This includes 4.9 billion in 2015 and 6.4 billion connected things in use in 2016 (about 7% from 2015). These numbers are fueled by major digital shifts by the forces of mobile, cloud computing, and social media combined with IoT. Many businesses feel that they are at a competitive disadvantage unless they pursue IoT. Gartner believes consumer applications will drive the number of connected things, while enterprises will account for most of the revenue. They estimate that 4 billion connected things will be in use in the consumer sector in 2016 and will reach over 13 billion in 2020 (Table 1.2). The automotive sector is also expected to show a very high growth rate (over 90% annually).

A separate analysis from Morgan Stanley believes that the number can actually be as high as 75 billion and also claims that there are 200 unique consumer devices or equipment that could be connected to the Internet.

Regardless of which study to agree with, the bottom line is that the stakes are high and people will be the beneficiaries of this new IoT economy. Using IoT-developed innovations, for example, we can reduce waste, protect our environment, boost farm production, get early warnings of structural weaknesses in bridges and dams, and enable remotely controlled lights, sprinkler systems, washing machines, sensors, actuators, and gadgets.

This revolution is based on the transformational role of digital technologies, in particular Internet-based cloud, mobility, and application technologies. But the real power of IoT is moving from an "open-loop" world characterized by people in the process to one that will be an automated "closed loop." In this model, humans will only intervene in the process as an exception, for example, if a robot, jet engine, driverless truck, or gas turbine require a part within itself to be changed (in some cases, even these will be automated!).

There's no reason to doubt that devices connected to IoT will soon be flooding the mass market. We'll see compact, connected sensors and actuators make their way onto everyday consumer electronics and household appliances and on general infrastructure.

Networks and semiconductor manufacturers no doubt will benefit from this movement, but big data vendors should also be cheering, with any and all things connected to the Internet that opens up more real-time data inventory to sell (Fig. 1.18).

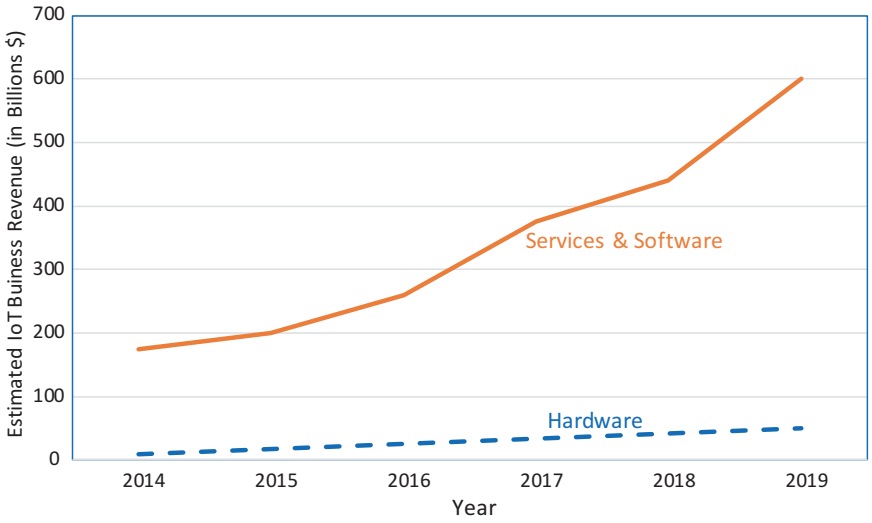


Fig. 1.18 IoT estimated business revenue from enterprise

1.4 History of the Internet

Before the advent of the Internet, the world's main communication networks were based on circuit-switching technology: the traditional telephone circuit, wherein each telephone call is allocated a dedicated, end-to-end, electronic connection between the two communicating stations (stations might be telephones or computers). Circuit-switching technology was not suitable for computer networking.

The history of the Internet begins with the development of electronic computers in the 1950s where the initial concepts of packet switching were introduced in several computer science laboratories. Various versions of packet switching were later announced in the 1960s. In the early 1980s, the TCP/IP (Transmission Control Protocol/Internet Protocol) stack was introduced. Then, the commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991, which made the Internet more popular and stimulated the rapid growth. The Web of Things (WoT), which based on WWW, is considered a part of IoT.

To illustrate the importance of packet-switching technologies, consider computer A (in Los Angeles) wants to communicate with Computer B (in New York) in a circuit-switched network. One common way is to select a path in the network connecting computers A and B. In this case, the selected path would be dedicated to A and B for the duration of their message exchange. The problem with circuit switching is that the line is tied up regardless of how much information is exchanged (i.e., no other computers are allowed to utilize the line between A and B even with free bandwidth). Unlike voice traffic, circuit switching is a problem for computers because their information exchange is typically "bursty" rather

than smooth or constant. Two computers might want to exchange a file, but after that file is exchanged, the computers may not engage in communication again for quite some time.

Packet switching was introduced as the alternative technology to circuit switching for computer communications. It has been reported that packet-switching work was done during the time of the Cold War, and a key part of motivation for developing packet switching was the design of a network that could withstand a nuclear attack. Such theory was denied by the Advanced Research Projects Agency Network (ARPANET), an early packet-switching network adopter and the first network to implement the Internet protocol suite TCP/IP. However, the later work on internetworking emphasized robustness and survivability, including the capability to withstand losses of large portions of the underlying networks.

To understand the fundamental of packet switching, consider sending a container of goods from Los Angeles to New York City. Rather than sending the entire container over a particular route, it is divided into packages (called packets). Packets are assembled, addressed, and sent in a particular way such that:

- The packets are numbered so they can be reassembled in the correct sequence at the destination.
- Each packet contains destination and return addresses.
- The packets are transmitted over the network of routes as capacity becomes available.
- The packets are forwarded across the network separately and do not necessarily follow the same route; if a particular link of a given path is busy, some packets might take an alternate route.

Packet switching is a generic philosophy of network communication, not a specific protocol. The protocol used by the Internet is called TCP/IP. The TCP/IP protocol was invented by Robert Kahn and Vint Cerf. The IP in TCP/IP stands for Internet protocol: the protocol used by computers to communicate with each other on the Internet. TCP is responsible for the data delivery of a packet, and IP is responsible for the logical addressing. In other words, IP obtains the address, and TCP guarantees delivery of data to that address. Both technologies became the technical foundation of the Internet.

The earliest ideas for a computer network, intended to allow general communications among computer users, were formulated by computer scientist J. C. R. Licklider of Bolt, Beranek, and Newman (BBN), in April 1963, in memoranda discussing the concept of the "Intergalactic Computer Network." Those ideas encompassed many of the features of the contemporary Internet. In October 1963, Licklider was appointed head of the Behavioral Sciences and Command and Control programs at the Defense Department's Advanced Research Projects Agency (ARPA). He convinced Ivan Sutherland and Bob Taylor that this network concept was very important and merited development, although Licklider left ARPA before any contracts were assigned for development [5].

Devices using the Internet must implement the IP stack. Packets that follow the IP specification are called IP datagrams. These datagrams have two parts: header

information and data. To continue with the letter analogy, think of the header as the information that would go on an envelope and the data as the letter that goes inside the envelope. The header information includes such things as total length of the packet, destination IP address, source IP address, time to live (the time to live is decremented by routers as the packet passes through them; when it hits zero, the packet is discarded; this prevents packets from getting into an "infinite loop" and tying up the network), and error checking information.

- The IP packets are independent of the underlying hardware structure. In order to travel across different types of networks, the packets are encapsulated into frames. The underlying hardware understands the particular frame format and can deliver the encapsulated packet.
- The TCP in TCP/IP stands for Transmission Control Protocol. This is a protocol that, as the name implies, is responsible for assembling the packets in the correct order and checking for missing packets. If packets are lost, the TCP endpoint requests new ones. It also checks for duplicate packets. The TCP endpoint is responsible for establishing the session between two computers on a network. The TCP and IP protocols work together.
- An important aspect of packet switching is that the packets have forwarding and return addresses. What should an address for a computer look like? Since it is a computer and computers only understand binary information, the most sensible addressing scheme is one based on binary numbers. Indeed, this is the case, and the addressing system used by IP version 4 software is based on a 32-bit IP address, and IP version 6 is based on 128-bit IP address as will be explained in Chap. 2 (Fig. 1.19).

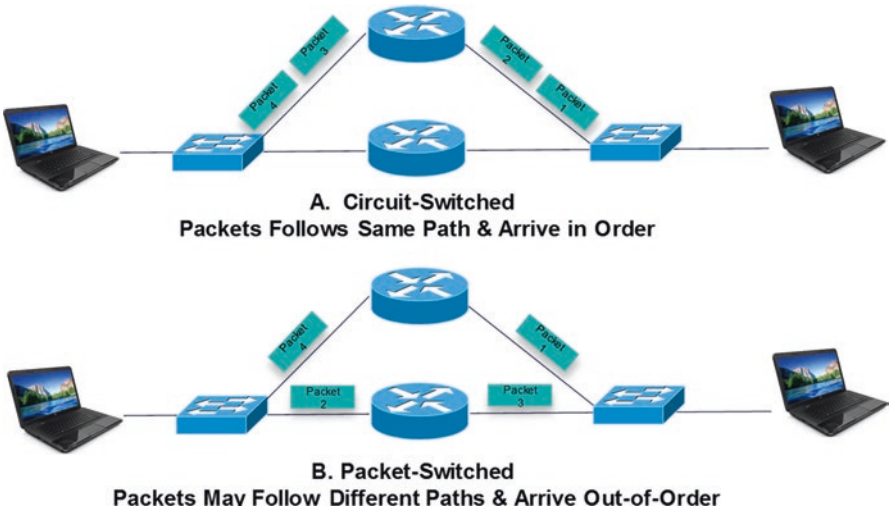


Fig. 1.19 Circuit switched vs. packet switched

1.5 Summary

We'd like to conclude this chapter by restating our definition of IoT as the network of things, with clear element identification, embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet. IoT is empowered by four main elements: sensors to collect information, identifiers to identify the source of data, software to analyze the data, and Internet connectivity to communicate and enable notifications. Sensors may be physical (e.g., sensors capturing the temperature) or logical (e.g., embedded software measurements such as CPU utilization). IoT's ultimate goal is to create a better environment for humanity, where objects around us know what we like, what we want, and what we need and act accordingly without explicit instructions.

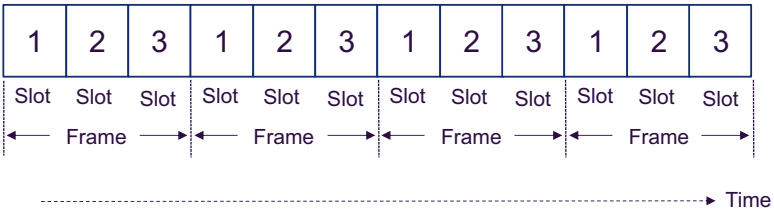
IoT is fueled by explosion in technologies including the IT and OT convergence; the introduction of Internet-based business at a fast rate; the explosion in smart mobile devices; the explosion in social networking applications; the overall technology explosion; the massive digital transformation; the enhanced user interfaces allowing people to communicate by a simple touch, voice command, or even an observing command; the faster than ever technology adoption; the increased demand for security applications and solutions; and of course Moore's Law. Securing IoT is viewed as a challenge and colossal business opportunity at the same time with areas that embrace securing the data at rest, securing the transport of the data, securing APIs/interfaces among systems and various sources of data, and of course controlling sensors and applications.

Problems and Exercises

1. What is the simple definition of IoT? What is the "more complete definition"? What's the main difference?
2. IoT components were listed for the simple definition to include the intersection of the Internet, Things, and data. Process and standards were added to the complete definition. Why are process and standards important for the success of IoT?
3. What are the main four components that empower IoT? List the main function of each component.
4. What is IoT's promise? What is IoT's ultimate goal?
5. Cisco estimated that the IoT will consist of almost 30 billion objects by 2020. Others have higher estimates. What was their logic?
6. What is Moore's Law? When was it first observed? Why is it relevant to IoT?
7. In a table, list the 12 factors that are fueling IoT with a brief summary of each factor.
8. What are the top three challenges for IoT? Why are those challenges also considered as opportunities?

9. What is BYOD? Why is it considered a security threat for the network?
10. How do companies deal with BYOD today? List an example of BYOD system.
11. Why is operation technology (OT) under pressure to integrate with information technology (IT)?
12. Uber is using smartphone Gyrometer data to monitor speeding drivers. What is "Gyrometer"? How does it work? Where was it first used?
13. What is KISS? What are the top five principles for KISS user experience?
14. Section 1.3.10 stated the following three facts: (i) over the history of computing hardware, computer power has been doubling every 18 months, (ii) biggest networks we have today have millions of nodes and billions of connection, and (iii) a human brain has a hundred thousand billion nodes and a hundred trillion connections. It then stated that using (i)–(ii), in year 2015, a computer should be as powerful as a human brain in about 25 years! How did the author arrive at 25? How long would it take if the computer power was doubling every 2 years instead of 18 months and why?
15. What are the key four differences between Analytics 1.0, 2.0, and 3.0?
16. List examples of solutions that offer Analytics 3.0.
17. What are the top three befits of cloud computing? What do they mean?
18. In a table format, compare IaaS, PaaS, and SaaS. List an example for each.
19. What are the main differences between virtual machines and containers in virtualization? Provide an example of container technology. Which approach do you prefer and why?
20. List two main functions that TCP/IP protocol, the bread and butter of today's Internet.
21. Why do we need both TCP and IP protocols?
22. It is often said by User Experience Experts that the "Best Interface for a system is no User Interface." What does such statement mean? When does it typically apply? Provide an example in networking technologies.
23. This question has four parts:
    (a) What is circuit-switched technology? What is packet-switched technology?
    (b) What are circuit-switched networks and packet-switched networks used for? List an example of each use.
    (c) Why did we need packet-switched technology?
    (d) In a table, list three main differences between packet switching and circuit switching?
    (e) Which approach is better for the Internet and why?
24. What is a connection-oriented protocol? What is a connectionless protocol? Provide an example of each.
25. Some companies use the term IoE instead of IoT. What is their logic?
26. What is Cloud 1.0 and Cloud 2.0? What is the main difference between cloud 1.0 and cloud 2.0? How does machine learning differ from traditional approaches to extract business intelligence form the data?

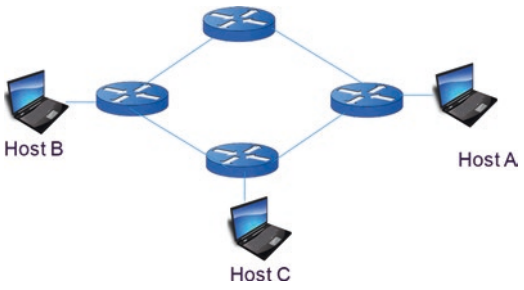
27. Circuit-switched networks are designed with either frequency-division multiplexing (FDM) or time-division multiplexing (TDM). For TDM link, time is divided into frames of fixed duration, and each frame is divided onto a fixed number of time slots as shown below (for a network link supporting up to three connections/circuits).



When the network establishes a connection across a link, the network dedicates one time slot in every frame to this connection. These slots are dedicated for the sole use of that connection, with one time slot available for use (in every frame) to transmits the connection's data.

(a) How does FDM work in circuit-switched networks?
(b) What is the typical frequency band in tradition circuit-switched-based telephone networks/public-switched telephone network (PSTN)?
(c) Compare FDM with TDM.
(d) Draw FDM and TDM for a tradition circuit-switched network link supporting up to five connections/circuits.

28. Refer again to problem 27 above. Let's assume that all links in the circuit-switched network are T1 (i.e., have a bit rate of 1.536 Mbps with 24 slots) and use TDM.



(a) Assuming setup and propagation delays are zero, how long does it take to send a file of 1.280M bits from Host A to Host B? How about from Host A to Host C? Do you expect the answer to be the same or different and why?
(b) Let's also assume that it takes 500 ms to establish an end–to-end circuit before Host A can begin to transmit the file and 250 ms for a propagation delay between

any two adjacent routers. How long does it take to send a file form Host A to Host B?

(c) What is the difference between transmission delay and prorogation delay? Which delay is a function of the distance between the routers?

References

1. A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, G. Schreier, The internet of things for ambient assisted living, in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, 2010*, pp. 804–809 Online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5501633
2. M Drobics, E Fugger, B Prazak-Aram, G Schreier, *Evaluation of a Personal Drug Reminder*. (unpublished, 2009)
3. S. Haller, S. Karnouskos, C. Schroth, *The Internet of Things in an Enterprise Context* (Springer (Berlin-Heidelberg), Vienna, 2008)
4. International Telecommunication Union. ITU Internet Reports 2005 and 2015:The Internet of Things. Geneva, s.n., 2005.http://www.itu.int/internetofthings/
5. K. Ashton, "That 'Internet of Things' Thing, In the real world, things matter more than ideas", June 22, 2009, Online: http://www.rfidjournal.com/articles/view?4986
6. Top 3 Security Issues in Consumer Internet of Things (IoT) and Industrial IoT Youtube John Barrett at TEDxCIT: https://www.youtube.com/watch?v=QaTIt1C5R-M
7. Wikipedia, ARPANET, Online: http://en.wikipedia.org/wiki/ARPANET
8. Gail Honda, Kipp Martin, Essential Guide to Internet Business Technology Book, Feb 19, 2002 by Prentice Hall, Online: http://www.informit.com/articles/article.aspx?p=27569&seqNum=4
9. http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz3YAtxfDCp
10. IoT Definitions, Online: http://gblogs.cisco.com/asiapacific/the-internet-of-everything-opportunity-for-anz-agribusiness/#more-120
11. Gartner News View: http://www.gartner.com/newsroom/id/2905717
12. Information Week IoE, Peter Waterhouse, ,December 2013, Online: http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-everything-connecting-things-is-just-step-one/d/d-id/1112958
13. *LG* Answers to IoT, the Latest Trend in IT -Talk Service-Oriented IoT, Online: http://www.lgcnsblog.com/features/answers-to-iot-the-latest-trend-in-it-talk-service-oriented-iot-1/
14. Driving Moore's Law with Python-Powered Machine Learning: An Insider's Perspective by Trent McConaghy PyData Berlin 2014, OnLine: http://www.slideshare.net/PyData/py-data-berlin-trent-mcconaghy-moores-law
15. Clock speed: Data from 1976–1999: E. R. Berndt, E. R. Dulberger, and N. J. Rappaport, "Price and Quality of Desktop and Mobile Personal Computers: A Quarter Century of History," July 17, 2000, http://www.nber.org/~confer/2000/si2000/berndt.pdf
16. Data from 2001–2016: ITRS, 2002 Update, On-Chip Local Clock in Table 4c: Performance and Package Chips: Frequency On-Chip Wiring Levels—Near-Term Years, p. 167. OnLine: http://www.singularity.com/charts/page62.html
17. Average transistor price: Intel and Dataquest reports (December 2002), see Gordon E. Moore, "Our Revolution," http://www.sia-online.org/downloads/Moore.pdf
18. The Internet of Things, Online: https://en.wikipedia.org/wiki/Internet_of_Things
19. L. David Roper, Silicon Intelligence Evolution: Online http://arts.bev.net/roperldavid , October 23, 2010, http://www.roperld.com/science/SiliconIntelligenceEvolution.htm
20. The Silicon Engine: A Timeline of Semiconductor in Computer, Online: http://www.computerhistory.org/semiconductor/timeline/1958-Mesa.html

21. T.E. Kurt, Disrupting and enhancing Healthcare with IoT, Health, Technology & engineering Program at USC, Arch 2, 2013, online: http://www.slideshare.net/todbotdotcom/disrupting-and-enhancing-healthcare-with-the-internet-of-things
22. Insight's The Semiconductor Laser's Cost Curve, Online: http://sweptlaser.com/semiconductor-laser-cost-curve
23. P. Welander "IT vs. OT: Bridging the divide - Traditional IT is moving more onto the plant floor. OT will have to accept a greater level of integration. Is that a problem or an opportunity?", Control engineering, 08/16/2013, Online: http://www.controleng.com/single-article/it-vs-ot-bridging-the-divide/db503d6cb9af3014f532cf19b5bf75e8.html
24. Airbnb Business Model, Online: https://www.quora.com/What-is-Airbnbs-business-model
25. Five Things You Can Learn From One of Airbnb's Earliest Hustles, Online: http://www.inc.com/alex-moazed/cereal-obama-denver-the-recipe-these-airbnb-hustlers-used-to-launch-a-unicorn.html
26. S. Ganguli, The Impact of the IoT on Infrastructure Monitoring, October 2015, Online: https://www.gartner.com/doc/3147818?srcId=1-2819006590&pcp=itg
27. Sqaure Inc, Online: https://en.wikipedia.org/wiki/Square,_Inc
28. G. Sterling, Greg, "Expanding Its Services, Square Launches Email Marketing With A Twist", April 2015, Online: http://marketingland.com/expanding-its-services-square-launches-email-marketing-with-a-twist-2-124282
29. Analysis of the Amazon Business Model, July 2015, Online: http://www.digitalbusinessmodelguru.com/
30. About Tesla, Online: http://www.teslamotors.com/about
31. A. Brisbourne, Tesla's Over The Air Fix: Best Example yet of the Internet of Things, February 2014, Online: http://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/
32. U. Wang, A Manufacturing Lesson From Tesla Motors, Forbes, August 2013, Online: http://www.forbes.com/sites/uciliawang/2013/08/08/a-manufacturing-lesson-from-tesla-motors/
33. How PayPal Here Stacks Up Against Other Mobile Payment Options, Online: http://mashable.com/2012/03/16/paypal-here-competitors/#cSQKd8eMwPqa
34. F. Richter, "Global Smartphone Traffic to Increase Tenfold by 2019", February 2015, Online: http://www.statista.com/chart/3227/global-smartphone-traffic-to-increase-tenfold-by-2019/
35. Security of IoT: Lessons from the Past for the Connected Future, Aa, Online: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
36. Curb Your Enthusiasm, Uber Newsroom, Joe Sullivan, Chief Security Officer, January 26, 2016
37. Fundamental Principles of Great UX Design | How to Deliver Great UX Design, Janet M. Six, Nov 17, 2014, Online: http://www.uxmatters.com/mt/archives/2014/11/fundamental-principles-of-great-ux-design-how-to-deliver-great-ux-design.php#sthash.oEzaPFAH.dpuf
38. Three Social Media Marketing Options to Consider in 2016, Hiral Rana, Jan 31, 2016, Online: https://www.google.com/search?q=social+media&rls=com.microsoft:en-US:IE-Address&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiU4_y107nMAhXFMKYKHXldAEAQ_AUICCgC&biw=1577&bih=912#imgrc=ZH-8cjbgp-pIBM%3A
39. Detecting a malfunctioning device using sensors, United States Patent 8777104, Online: http://www.freepatentsonline.com/8777104.html
40. Virtual Machines Vs. Containers: A Matter Of Scope, Information Week Network Computing, May 28, 2014, Online: http://www.networkcomputing.com/cloud-infrastructure/virtual-machines-vs-containers-matter-scope/2039932943
41. "Google's Self-Driving Car Hit a Bus", American Safety Council February 29, 2016, Online: http://blog.americansafetycouncil.com/googles-self-driving-car-hit-a-bus/
42. "10 Million Self-Driving Cars will be on the Road by 2020", Business Insider, Juley 29, 2015, Online: http://www.businessinsider.com/report-10-million-self-driving-cars-will-be-on-the-road-by-2020-2015-5-6

43. “How Self-driving Cars work”, Shima Rayej, Robohub Automotive, June 3, 2014, Online: http://robohub.org/how-do-self-driving-cars-work/
44. Alternative To, NetCrunch, Online: http://alternativeto.net/software/netcrunch/comments/
45. Amazon Web Services is Approaching a $10 billion-a-year business, Recorde, April 28 2016, Online: http://www.recode.net/2016/4/28/11586526/aws-cloud-revenue-growth
46. Google says welcome to the Cloud 2.0, ComuterWold, May 24, 2016 issue, Online: http://www.computerworld.com/article/3074998/cloud-computing/google-says-welcome-to-the-cloud-20.html?token=%23tk.CTWNLE_nlt_computerworld_enterprise_apps_2016-05-27&idg_eid=28bc8cb86c8c36cb5f0c09ae2e86ba26&utm_source=Sailthru&utm_medium=email&utm_campaign=Computerworld%20Enterprise%20Apps%202016-05-27&utm_term=computerworld_enterprise_apps#tk.CW_nlt_computerworld_enterprise_apps_2016-05-27
47. “Gartner Says 6.4 Billion Connected "Things “Will Be in Use in 2016, Up 30 Percent From 2015”, November 10, 2015, online: http://www.gartner.com/newsroom/id/3165317
48. Cisco Visual Networking Index: Forecast and Methodology, 2015–2020, June 6, 2016, Online: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html