# Chapter 1

# The Third ICT Wave

## 1.1 Rise of the Machines

Over the past decades, billions of people have hooked themselves up to the Internet via the computer, and more recently mobile devices such as smartphones. This communication revolution is now extending to objects as well as people. Machine-to-machine (M2M) communication has long been predicted, and now it is rushing into the present. According to Parks Associates, the number of smartphones (excluding feature phones) worldwide is expected to top 1.1 billion in 2013. However, this is just the tip of the iceberg. Smart grid devices will reach 244 million; e-readers and tablets will be 487 million; networked office devices, 2.37 billion; networked medical devices, 86 million; connected automobiles, 45 million; connected appliances, 547 million; connected military devices, 105 million; information technology (IT) system devices, 431 million; connected supervisory control and data acquisition (SCADA)/industry automation devices, 45 million; and other connected consumer electronic devices minus smartphones, e-readers, and tablets will reach a whopping 5+ billion and counting.

"Rise of the machines" became a popular catchphrase after *Terminator 3: Rise of the Machines*, a 2003 science-fiction action film directed by Jonathan Mostow and starring Arnold Schwarzenegger. The movie demonstrates the power of machines or robots that could potentially overpower human beings.

During the first decade of the twenty-first century, big U.S. defense budgets financed the deployment of thousands of service robots, including unmanned aerial and underwater vehicles, to Iraq and Afghanistan. *IEEE Spectrum* [1] estimated a million industrial robots toiling around the world in 2008, and Japan is where they're the thickest on the ground. In 2011, the world's industrial robot population was estimated to be 1.2 million. Also, according to the Frankfurt-based International Federation of Robotics, the service robot market is expected to double in size by 2013 from 2011 [2].

A robot is a kind of tightly coupled cyber-physical system (CPS) [4,165]. A CPS (Figure 1.1) is an embedded sensor network and control system featuring a tight combination of, and coordination between, the system's computational and physical elements. Cyber-physical systems or robots can be found in areas as diverse as aerospace, automotive industry, chemical


**Figure 1.1 Cyber-physical system (CPS).**

processes, civil infrastructure, energy, healthcare, manufacturing, transportation systems, entertainment, and consumer appliances. A real-world example of such a system is the Massachusetts Institute of Technology (MIT) CarTel project where a fleet of taxis collects real-time traffic information in the Boston area. Together with historical data, this information is then used for calculating the fastest route for a given time of the day.

The U.S. National Science Foundation (NSF) has identified cyber-physical systems as a key area of research, proposed by Helen Gill at the High Confidence Software and Systems conference [28] in 2008. In 2007, the President's Council of Advisors on Science and Technology listed CPS as one of the top eight key technologies of the future, and a $4 billion budget was allocated for the Networking and Information Technology Research and Development [29] project. The expectation is that in the coming years, ongoing advances in science and engineering will improve the link between computational and physical elements, dramatically increasing the adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of cyber-physical systems.

The power of machines has experienced rapid development, first through the steam-engine technology based industrial revolution and then the second electrical, oil-powered internal combustion engine industrial revolution. Along with the rise of the power of machines comes the exponential rise of the number of machines during the ongoing third industrial revolution of the Internet-based information age. The past three decades have seen extraordinary growth in the number and choice of electrical and electronic machines or devices (Figure 1.2) [3].

The so-called Internet of Things (IoT), together with cloud computing, is, after the modern computer (1946) and the Internet (1972), the world's third wave of the information and communications technology (ICT) industry. Gordon Bell's law

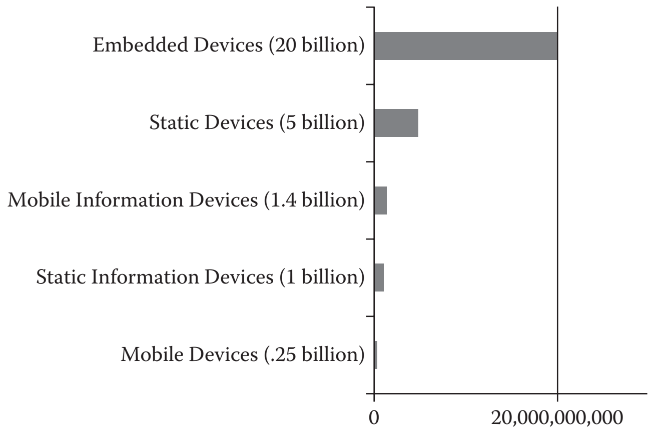


**Figure 1.2 Number of intelligent devices.**

says that "roughly every decade a new, lower priced computer class forms based on a new programming platform, network, and interface resulting in new usage and the establishment of a new industry" [271]. Bell predicted that home and personal area networks will form starting from 2010.

Also, in 2002, Sun's chief technology officer Greg Papadopoulos indicated that the first Internet wave consisted of an "Internet of computers" and the second wave, which we are currently in, is an "Internet of Things that embed computers." The third Internet wave, which is an "Internet of Things," consists of physical objects like thermostats, switches, packages, and clothes.

So far, our view of the Internet has been human-centric. It is quite likely that sooner or later the majority of items connected to the Internet will not be humans, but things. The IoT will primarily expand communication from the 7 billion people around the world to the estimated 50 to 70 billion machines. This means significant opportunities for the telecom industry to develop new IoT "subscribers" that substantially surpass the number of current subscribers based on population.

This advancement signifies a massive shift in human development, from an electronic society to a ubiquitous society in which everything is connected (for example, the sensor in Nike+ shoes sends information to an iPod application [192]) and everything can be accessed anywhere. Supported by IPv6 and eventually the Future Internet Architecture, the IoT would have the potential of connecting the 100 trillion things that are deemed to exist on Earth [17].

Recent developments predict that we will have 16 billion connected devices by the year 2020 [5], which will average out to six devices per person on earth. Devices like smartphones and M2M or thing-to-thing communication will be the main drivers for further development.

Cisco's Dave Evans has posted a great infographic (http://blogs.cisco.com/news/the-internet-of-things-infographic/) showing that communicating *things*, essentially embedded sensors, have already outstripped the number of communicating *homo sapiens* in 2010. Future historians will probably look back at 2010 as the year when Internet-connected devices like digital picture frames, web-connected global positioning system devices, and broadband TVs came online in greater numbers than new human subscribers. Electricity meters, dishwashers, refrigerators, home heating units, and several other objects with tiny sensors are next in line.

By 2015, wirelessly networked sensors in everything we own will form a new web. But it will only be of value if the terabyte torrent of data it generates can be collected, analyzed, and interpreted [6]. The first direct consequence is the generation of huge quantities of data from physical or virtual objects that are connected. As a result, consumer-device-related messaging volume could easily reach between 1,000 and 10,000 per person per day [7,8].

As a key aspect of the next-generation Internet, the Internet of Things is expected to have a dramatic impact on almost all sectors of the web-based service economy. It will enable tremendous efficiency gains, especially in the transportation, retail, manufacturing, logistics, and energy sectors. The world market for Internet of Things–related technologies, products, and applications alone will increase significantly from $2 billion today to more than $11.5 billion in 2012, with average annual growth rates of almost 50 percent [269]. More aggressive forecasts predict a market volume of more than $27 billion in 2011 [270]. Forrester Research also predicts that the number of objects connected to the IoT will be 30 times the number of people connected to the Internet by 2020. IoT is a trillion-dollar industry.

## 1.2 The IoT Kaleidoscope

Although the concept of IoT was expressed in the form of "computers everywhere" by professor Ken Sakamura (University of Tokyo) in 1984 and "ubiquitous computing" by Mark Weiser (Xerox PARC) in 1988, the phrase *Internet of Things* was coined by Kevin Ashton (Procter & Gamble) in 1998 [9] and developed by the Auto-ID Center of MIT from 2003. Ashton then described the IoT as "a standardized way for computers to understand the real world." MIT has also contributed significant research in this field, notably Things That Think consortium at the Media Lab and the CSAIL effort known as Project Oxygen. Other major contributors include Georgia Tech's College of Computing, New York University's Interactive Telecommunications Program, University of California at Irvine's Department of Informatics, Microsoft Research, Intel Research and Equator, and Ajou University UCRi and CUS.

The concept of IoT has since become popular through the radio-frequency identification (RFID) Auto-ID Center's six research labs in the United States, United Kingdom, Australia, Switzerland, Japan, and China. It refers to uniquely identifiable objects and their virtual representations in an Internet-like architecture. Although the idea is simple, its application is powerful. If all objects of daily life were equipped with radio tags, they could be identified and inventoried by computers

[10,11], and daily life on our planet could undergo a drastic transformation [12].

In the International Telecommunication Union (ITU) Internet report of 2005 [13] and the EPOSS's (European Technology Platform on Smart Systems Integration) IoT 2020 report [22], however, the concept of IoT was further extended to cover a plethora of technologies, applications, and services beyond RFID and the aforementioned CPS, which will enhance quality of life while providing new revenue opportunities for a host of enterprises. The Internet as we know it is transforming radically, from an academic network in the 1980s and early 1990s to a mass-market, consumer-oriented network. Now, it is set to become fully pervasive, connected, interactive, and intelligent. Real-time communication is possible not only by humans but also by things at any time and from anywhere.

Over two decades ago, the late Mark Weiser of Xerox PARC developed a seminal vision of future technological ubiquity—one in which the increasing *availability* of processing power would be accompanied by its decreasing *visibility*. As he observed, "the most profound technologies are those that disappear … they weave themselves into the fabric of everyday life until they are indistinguishable from it" [272]. Weiser is widely considered to be the father of *ubiquitous computing*, a term he coined in 1988.

According to Weiser, "Ubiquitous computing names the third wave in computing, just now beginning. First were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, or the age of calm technology, when technology recedes into the background of our lives." *Pervasive computing* is a similar term used by IBM's former chief executive officer (CEO) Louis Gerstner in 1996, when I joined IBM as a software programmer doing job-scheduling software development in the SP PowerParallel Division that built the world's fastest supercomputer at the time, ASCI-Blue Pacific.

Just like CPS, ubiquitous computing is synonymous with or closely related to IoT. About a dozen other terms are synonymous with or closely related to IoT, which can be regarded as an umbrella word to cover the technologies and applications that these terms or phrases describe. A comprehensive (but not complete due to the ever-changing nature of technology developments) collection of those terms and phrases is listed and explained in the following paragraphs.

M2M (machine-to-machine) refers to technologies that allow both wireless and wired devices to communicate with each other or, in most cases, a centralized server. An M2M system uses devices (such as sensors or meters) to capture events (such as temperature or inventory level), which are relayed through a network (wireless, wired, or hybrid) to an application (software program) that translates the captured events into meaningful information (such as the statistics of a vehicle's usage in OnStar). M2M communication is a relatively new business concept, born from the original telemetry technology, utilizing similar technologies but modern versions of them.

Telemetry is a technology that allows remote measurement and reporting of information. Systems that need external instructions and data to operate require the counterpart of telemetry, telecommand. Many modern telemetry systems take advantage of the low cost and ubiquity of GSM networks by using SMS to receive and transmit telemetry data. Telemetry has unlimited applications in many fields including meteorology, space science, agriculture, water management, defense, resource exploration, rocketry, medicine, and so on.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, and to cooperatively pass their data through the network to a main location. The more modern networks are bidirectional, becoming wireless sensor and actuator networks (WSANs) enabling the control of sensor activities.

In 2008, IBM's CEO Sam Palmisano outlined a new agenda for building a "smarter planet" during a speech [14] at the Council on Foreign Relations. The IBM initiative seeks to highlight how forward-thinking leaders in business, government, and civil society around the world are capturing the potential of smarter systems to achieve economic growth, efficiency, sustainable development, and societal progress. Examples of smarter systems include smart grids, water management systems, solutions to traffic congestion problems, and greener buildings. These systems have historically been difficult to manage because of their size and complexity. But with new ways of monitoring, connecting, and analyzing the systems, business, civic, and nongovernmental leaders are developing new ways to manage these systems. The IBM initiative was embraced by President Obama [15] and Smarter Earth became a U.S. government initiative. A $3.4 billion grant for smart grid was announced by President Obama later in 2009 [16]. Smart Grid is poised to "change" the energy efficiency management landscape.

In November 2008, *Time* magazine listed the IPSO (Internet Protocol for Smart Objects) Alliance and the Internet of Things among the most important innovations of 2008. Also in 2008, the U.S. National Intelligence Council published a report titled, "Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests out to 2025." These technologies are biogerontechnology, energy storage materials, biofuels and bio-based chemicals, clean coal technologies, service robotics, and the Internet of Things. With regard to the Internet of Things, it stressed the following:

> By 2025 Internet nodes may reside in everyday things—food packages, furniture, paper documents, and more. Today's developments point to future opportunities and risks that will arise when people can remotely control, locate, and monitor even the most mundane devices and articles. Popular demand combined with technology advances could drive

> widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development and military capability. [194]

Many U.S. companies are involved and playing important roles, with information technology (IT) giants such as IBM focusing on applications, Cisco on infrastructures, and so on.

Some experts predict that the IoT will help tackle two of the biggest problems facing mankind today: energy and healthcare. Currently buildings waste more energy than they use effectively, but we will be able to cut this waste down to almost nothing. Currently we make visits to our general practitioner twice a year, at most, but we will be able, thanks to a few sensors discreetly attached to our body, to continuously monitor our vital functions. Those two issues are among the top of President Obama's agenda. In 2009, Obama reiterated [20] his commitment to healthcare reform and stood firm on his assertion that healthcare IT must to be at the crux of reform. *Telehealth* or *telemedicine* are terms that are related to IoT.

In *Shaping Things*, the latest book by world-renowned science-fiction writer and futurist Bruce Sterling [27], ideas are outlined for *spime*, a word the author coined in 2004. A spime is, by definition, the protagonist of a documented process. It is a historical entity with an accessible, precise trajectory through space and time. It can also be a form of ubiquitous computing that gives smarts and searchability to even the most mundane of physical products. Imagine losing your car keys and being able to search for them with Google Earth. The three facets of spime that are relevant to IoT are as follows:

- Small, inexpensive means of remotely and uniquely identifying objects over short ranges
- A mechanism to precisely locate something on Earth
- A way to mine large amounts of data for things that match some given criteria

More recent ideas have driven the IoT toward an all-encompassing vision to integrate the real world into the Internet—the real-world Internet (RWI) [163]. RWI and IoT are expected to collaborate with other emerging concepts such as the Internet of services (IoS), and the building block of parallel efforts such as the Internet of energy (IoE) is expected to revolutionize the energy infrastructure by bringing together IoS and IoT/RWI. It is clear that the RWI will heavily impact the way we interact in the virtual and physical worlds, overall contributing to the effort of the future Internet.

Other terms or phrases that are relevant but more academic include sentient computing, haptic computing, physical computing, ambient intelligence, context-aware computing [18], things that think, autonomic computing, machine that talks, everyware [19], network embedded devices [170], domotics, and so on.

As you can see, the IoT-related terms come in different shapes and forms; a kaleidoscope-like picture [74] of IoT-relevant terms and phrases is shown in Figure 1.3. Despite the technology existing in its various forms, IoT comprises of a number of separate technologies that need to be mixed and matched in the appropriate manner to enable a broad market deployment.


**Figure 1.3 IoT-related terms.**

## 1.3 Defining Internet of Things

The IoT is a concept that has received considerable and significant attention and support within the European Commission (EC) with respect to strategic developments for ICT and the Information Society. Viviane Reding, vice president of the EC, in a speech to the Future of the Internet initiative of the Lisbon Council identified the IoT as an important driver for the Internet of the future [5].

An EC communication to the European Parliament, the Lisbon Council, the European Economic and Social Committee, and the Committee of the Regions entitled "Internet of Things: An Action Plan for Europe" was adopted on June 18, 2009, and reinforces the commitment to the concept and its importance for Europe, quoting the following in its conclusions [11]:

> Internet of Things (IoT) is not yet a tangible reality, but rather a prospective vision of a number of technologies that, combined together, could in the coming 5 to 15 years drastically modify the way our societies function. By adopting a proactive approach, Europe could play a leading role in shaping how IoT works and reap the associated benefits in terms of economic growth and individual well-being, thus making the Internet of Things an Internet of Things for people.

In China, a number of significant public speeches about IoT were delivered in the second half of 2009. On August 7, Chinese Premier Wen Jiabao made a speech in the city of Wuxi calling for the rapid development of Internet of Things ("Sensing China" was the term in Chinese he used to refer to what the IoT technologies should be used for) technologies (Figure 1.4). Rapidly, an "IoT wave" spread across the nation. IoT became a buzzword instantaneously in China. Government officials at all levels, as well as the rank and

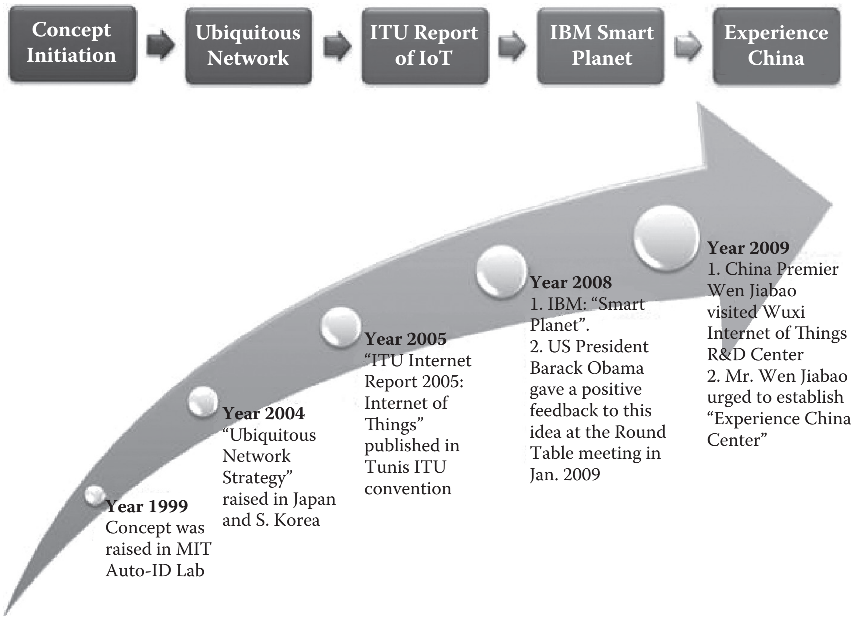


**Figure 1.4 IoT development.**

file, began trying to understand what the Internet of Things is. More than 60 books on this topic have been published in China since 2010.

Wen Jiabao followed up with another speech on November 3 at the Great Hall of the People in Beijing, in which he called for breakthroughs in wireless sensor networks and the Internet of Things. IoT was written into Premier Wen's "government work report" during the National People's Congress and the Chinese People's Political Consultative Conference in 2010, and the development of IoT industry became a national strategy. As a consequence, IoT was also written into the nation's "Twelfth Five-Year" plan in 2011. In response to the central government's initiative, over 60 related alliances and consortia were formed throughout China. Since 2009 [167], IoT has almost become a household buzzword (Figure 1.5).

The Chinese believe that China missed the first two waves of the ICT (information and communications technology) industry developments. Now, though, China may be well

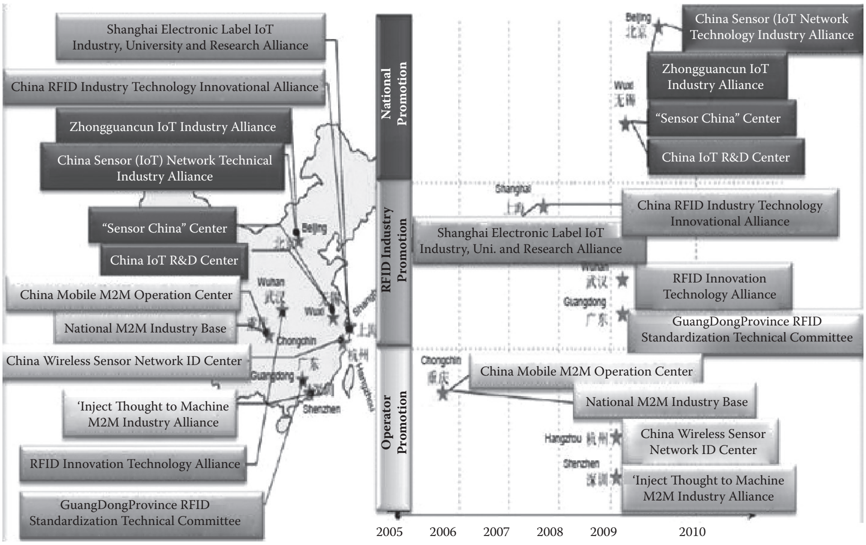


**Figure 1.5 IoT development in China.**

poised to take part or even lead in the third IoT wave based on the leapfrogging theory [23]. The fact is that China has the largest customer base, newer ICT infrastructure, and a determined and centralized government that has the almighty power of allocating and consolidating (top-down instructional planning versus bottom-up endless democratic debating/hearing in the Western world) national resources. IoT is more about infrastructure at the current stage than about income-generating, innovative business models. Figure 1.6 shows a SWOT (strengths, weaknesses, opportunities, and threats) analysis of China's IoT initiative and development [74].

In Japan and Korea, the buzzword is *ubiquitous* computing or the letter u as a prefix to a number of words such as u-Korea, u-Japan, u-city, u-home, u-tourism, u-business, u-defense, u-government, to name a few, rather than IoT, but these refer to the same thing. The u-words are sprinkled all over presentations, descriptions, and reports. There is a ubiquitous economy and the ubiquitous society; to sum everything up, there is u-life. The u-fever started around 2004 when the

SWOT Analysis of China's Advantage of IoT Development

| | **Positive** | **Negative** |
|---|---|---|
| **Internal Factors** | **Strength**<br>• IoT is a national strategy<br>• Power of centralized government<br>• Fast economic growth<br>• Nationwide support<br>• Largest customer base<br>• World-class newer infrastructure<br>• Lower labor costs<br>• Lots of money to invest | **Weakness**<br>• Underdeveloped middleware industry<br>• Experience in standardization<br>• Underdeveloped sensor technologies<br>• Software recognition and capabilities<br>• Top-notch talents<br>• International business development<br>• Repeat low-tech works<br>• Waste of resources |
| **External Factors** | **Opportunities**<br>• At the same start-line with peers<br>• Leapfrogging advantages<br>• Standardization opportunities<br>• Economic stagnation outside<br>• Lack of focus in US<br>• Hard to consolidate in Western nations<br>• Higher labor costs in Western nations | **Threats**<br>• Better international products<br>• Not owner of major standards<br>• Lack of industry giants<br>• Loss of talents to foreign competitors<br>• National security concerns |

**Figure 1.6 SWOT analysis of China's IoT.**

term M2M become popular in the United States. Before the *u* (ubiquitous) era was the *e* (electronic) era. The *e* era is concerned with the acceptance of digital communication for legally binding information. The *u* era proceeds to include objects, not humans only, in the circle of information producers and consumers [21].

Although the terms *Internet of Things* or *ubiquitous computing* were coined by Americans, they didn't become as popular in the United States. As mentioned before, the slogans "smarter planet" or "wisdom of Earth" were proposed by IBM, which again seized the Zeitgeist and told the right story at the right time to the right people in the depth of economic recession and financial crisis as well as climate change and global warming challenges. These were adopted by President Obama, who is trying find a dotcom-like innovation that could catalyze new markets for sustainable growth and save the economy. "Smarter planet" and "wisdom of Earth" refer to almost the same thing as IoT or u-life. Terms like *smart earth*, *smart grid*, *smart home*, *smart city*, and so on are more widely used in the United States, which indicates that the U.S. people as a whole think in terms of "smarter."

This is perhaps a coincidence but it isn't a joke. People in the United States seem more practical and tend not to follow what the government or an authority (such as EC) says. Some in the United States think IoT is the Internet of European things (and jokingly call the European Parliament the "Parliament of Things" [164]): a fiasco, or a big concept with no substance. That's probably why IoT is not a buzzword in the United States, like cloud computing, software as a service (SaaS), SOA, and others. Instead, *connectivity* is becoming a more popular term after M2M that refers to the same thing as IoT but more to the "real matter" and innovative new business model creations. However, we should not forget that the Europeans invented the Web. It seems that they are now on track to make the Internet of European Things into the Internet of Real Things, according to Viviane Reding [162].

Nevertheless, the *Internet of Things* is arguably still the most comprehensive term to describe the all-inclusive contents that the aforementioned terms and phrases refer to. This book is trying to raise awareness and acceptance of the term *Internet of Things* in the United States as well as elsewhere in the world. But what is the Internet of Things?

Due to the multifaceted, all-inclusive nature and scope of the Internet of Things, it's almost impossible to have a definition that everyone agrees on. IoT means different things to different people, just like the story about the six blind men and the elephant.

Below are a few definitions of the Internet of Things, and most come from Europe.

- CASAGRAS's (Coordination and Support Action for Global RFID-related Activities and Standardization) IoT definition:

  IoT is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability [24].

- SAP's IoT definition:

  IoT is going to create a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these "smart objects" over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues [25].

- EPoSS's (the European Technology Platform on Smart Systems Integration) IoT definition:

  The network formed by things/objects having identities, virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate with the users, social and environmental contexts [22].

- CERP's (Cluster of European RFID Projects) IoT definition:

  Internet of Things is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. In the IoT, "things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these "smart things" over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues [26].

The definition of IoT depends very much from the aspect or angle examined. The aforementioned definitions are mostly from an RFID point of view. A comprehensive, all-inclusive view should be sought.

- IoT definition or statement of this book (Figure 1.7):

  The Internet of Things is a plethora of technologies and their applications that provide means to access and control all kinds of ubiquitous and uniquely identifiable devices, facilities, and assets. These include equipment that has inherent intelligence, such as transducers, sensors, actuators, motes [179], mobile devices, industrial controllers, HVAC (heating, ventilation, and air-conditioning) controllers, home gadgets, surveillance cameras, and others, as well as externally enabled things or objects, such as all kinds of assets tagged with RFID, humans, animals, or vehicles that carry smart gadgets, and so forth. Communications are via all sorts of long- and

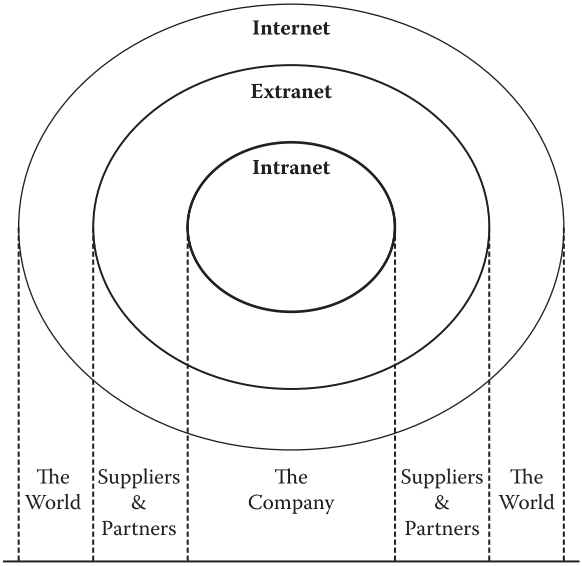


**Figure 1.7 Intranet/Extranet/Internet.**

short-range wired or wireless devices in different kinds of networking environments such as Intranet, extranet, and Internet that are supported by technologies such as cloud computing, SaaS, and SOA and have adequate privacy and security measures, based on regulated data formats and transmission standards. The immediate goal is to achieve pervasive M2M connectivity and grand integration and to provide secure, fast (real time), and personalized functionalities and services such as (remote) monitoring, sensing, tracking, locating, alerting, scheduling, controlling, protecting, logging, auditing, planning, maintenance, upgrading, data mining, trending, reporting, decision support, dashboard, back office applications, and others. The ultimate goal is to build a universally connected world that is highly productive, energy efficient, secure, and environment friendly.

## 1.4 IoT: A Web 3.0 View

The Internet (network) and the web (application) are two sides of a coin. The Internet was invented by Vinton Cerf in 1973, and the invention of the web in 1989 was credited to Tim Berners-Lee and later caught worldwide attention by Marc Andreessen's Mosaic web browser in 1992. The Internet (hardware) is the infrastructure and the web (software) is the application everybody uses. Just like the Internet revolution, in the Internet of Things, web-based applications and software (the supporting data representation and middleware) are the keys.

McKinsey [36] summarized the key application functionalities of IoT systems:

1. Information and analysis
   a. Tracking behavior
   b. Enhanced situational awareness
   c. Sensor-driven decision analytics
2. Automation and control
   a. Process optimization
   b. Optimized resource consumption
   c. Complex autonomous systems

According to Harbor Research, the web-based applications, systems, and networked services of smart systems or IoT are expanding more rapidly than the hardware and infrastructure [37]. This means the software (middleware and web-based integrated applications) market will play a pivotal role in the IoT business.

As is well known, Web 1.0 is about publishing and pushing content to the users. It's mostly a unidirectional flow of information. The shift from Web 1.0 to Web 2.0 can be seen as a result of technological refinements as well as the behavior change of those who use the World Wide Web, from publishing to participation, from web content as the outcome of large up-front investment to an ongoing and interactive process. Web 2.0 is about two-way flow of information and is associated with web applications that facilitate participatory information sharing, interoperability, user-centered design, and collaboration. Example applications of Web 2.0 include blogs, social networking services (SNSs), wikis, mashups, folksonomies, video-sharing sites, massive multiplayer online role-playing games, virtual reality, and so on.

Enterprise 2.0 is the use of Web 2.0 technologies within an organization to enable or streamline business processes while enhancing collaboration (Figure 1.8). It is the extension of Web 2.0 into enterprise applications. IoT technologies and applications can be integrated into Enterprise 2.0 for enterprises that need to monitor and control equipment and facilities and integrate with their ERP and CRM back office systems.

Definitions of Web 3.0 vary greatly. Many believe that its most important features are Semantic Web and personalization; some argued that Web 3.0 is where the *computer* is generating new information rather than the human.

The term Semantic Web was coined by Tim Berners-Lee, the inventor of the World Wide Web. He defines the Semantic Web as "a web of data that can be processed directly and indirectly by machines." Humans are capable of using the web to carry out tasks such as reserving a library book or searching



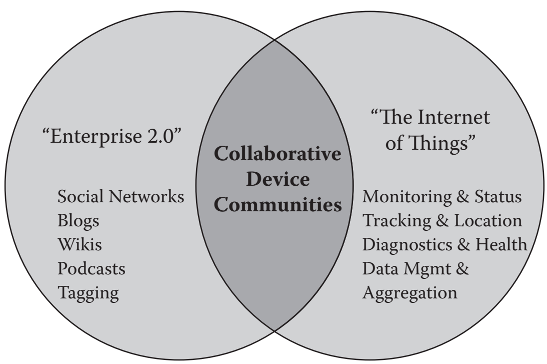


**Figure 1.8 Blending of IoT and Enterprise 2.0.**

for a low price for a DVD. However, machines cannot accomplish all of these tasks without human direction, because web pages are designed to be read by people, not machines. The Semantic Web is a vision of information that can be readily interpreted by machines, so machines can perform more of the tedious work involved in finding, combining, and acting upon information on the Web.

Some consider the Semantic Web an unrealizable abstraction and see Web 3.0 as the return of experts and authorities to the Web. I share the same thought. If there is no tangible difference but only a conceptual one, the concept of Semantic Web–based Web 3.0 doesn't stand on solid ground. Rather, the Web 3.0 of machine-generated data is more practical, makes more sense, and is possible to implement.

While Web 3.0 arguments are not yet settled, some people have started talking about Web 4.0 [30], the ubiquitous Web.

A fundamental difference between the Internet of People (Web 1.0 and Web 2.0) and the Internet of Things is that in the former, data are generated by people (keyed in by hand, photographed by hand, etc.); in the latter, data are generated by machines, not humans. This difference makes it enough to start a new version of the World Wide Web, or Web 3.0. The data are generated by things and consumed by people and machines via SaaS or XaaS (Everything as a Service), and this model constitutes the basis of Web 3.0 as depicted in Figure 1.9 [74]. We choose to use the term Web 3.0 instead of Web 4.0 based on the concept of machine-generated data in addition to the Semantic Web, which seems to not have much substance up to now. It is too much of a jump to go to Web 4.0.

## 1.5 Summary

After decades of fast-paced development, telecom networks worldwide now basically satisfy the need for man-to-man

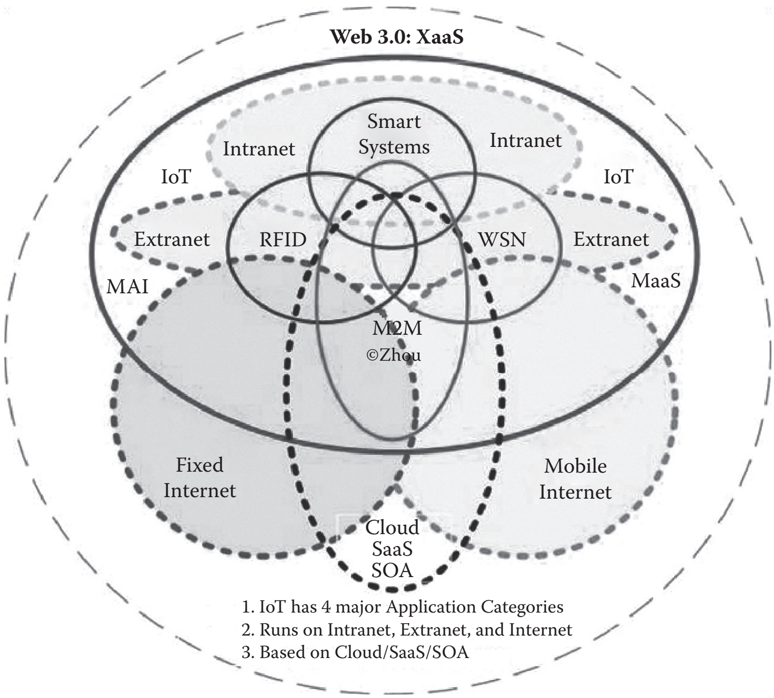


**Figure 1.9 Web 3.0: The Internet of Things.**

communication anywhere and at any time. However, new demand has arisen for machine-to-machine and machine-to-man, or the Internet of Things, communications. The development of these M2M technologies has attracted greater attention in recent times in light of the "smart Earth" and "Sensing China" concepts proposed by the American and Chinese governments and other parts of the world such as the European Union following the global financial crisis. According to Forrester Research, by 2020 machine-to-machine data exchange will be 30 times greater than the number of exchanges between people. M2M or IoT is therefore considered the next trillion-dollar segment of the international telecom market.

The physical world itself is becoming a connected information system. In the world of the Internet of Things, sensors and actuators embedded in physical objects are linked through wired and wireless networks that connect the Internet. These information systems churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding the complexity of the real world and responding to it swiftly.

The Internet of Things and related concepts, terms, and phrases and their potentially vast scope of applications as well as their impacts on business and social life were described in this chapter. The definitions of IoT were described and the author also gave his own definition and understanding, which will be the foundation of the book.

In the next chapter, a more detailed, panoramic view of IoT applications will be introduced and a few concrete vertical applications will be described in greater detail.