International Journal of Business and Economics Research
2017; 6(5): 115-123
http://www.sciencepublishinggroup.com/j/ijber
doi: 10.11648/j.ijber.20170605.15
ISSN: 2328-7543 (Print); ISSN: 2328-756X (Online)

The Internet of Things: Economic and Industrial Dimensions

Hans Werner Gottinger

Strategic Economics, STRATEC Consulting, Munich, Germany

Email address:
stratec_c@yahoo.com

To cite this article:
Hans Werner Gottinger. The Internet of Things: Economic and Industrial Dimensions. *International Journal of Business and Economics Research*. Vol. 6, No. 5, 2017, pp. 115-123. doi: 10.11648/j.ijber.20170605.15

Received: August 21, 2017; **Accepted**: September 11, 2017; **Published**: October 30, 2017

Abstract: The paper shows how the Internet has moved to a radical expansion with the Internet of Things (IoT) with everything being connected up to a scale of aggregate capacity and complexity. It could evolve into a network where not only each node could be a computational device but by itself would also be an intelligent computing device that could replace human supervision and control as through Artificial Intelligence (AI). The Internet of Things (IoT) as being embedded in the 'Industrial Internet' (IIoT) is a new paradigm shift that comprehensively affects computers and networking technology. In German industry and beyond this is referred to as 'Industry 4.0'. This technology is going to increase utilization and diversified connectivity followed by Bandwidth of the Internet. More and more (intelligent) devices in this network are connected to the Internet through various combinations of sensor networks.

Keywords: Internet of Things, Industrial Internet, Internet Technologies, Innovation, Artificial Intelligence, Security, Economic Benefits

1. Introduction

Over a few decades, the Internet has been in a constant state of evolution. The early days of the Internet were characterized by the World Wide Web, a network of linked

Hypertext Markup Language (HTML) documents that resided on top of the Internet architecture. This network of static HTML pages gradually evolved into what is referred to as Web 2.0, in which two-way communication became common, which enabled user participation, collaboration and interaction. Web 2.0 technologies include social networking services - technologies that have become essential to modern social interaction as well as for global business. While Web 2.0 currently dominates the Internet, network engineers have been working towards another goal, commonly referred to as the Semantic Web and sometimes referred to as Web 3.0. The goal of the Semantic Web (embracing pertinent artificial intelligence techniques such as machine learning with deep learning through neural networks) is to mark up web content in a way that makes it understandable by machines, allowing machines and search engines to behave more intelligently. Marking up web content in standardized formats would allow machines to process and share data on their own, without the need for human mediation. Alongside developments in Internet technologies, technologies in Sensor Networks and Near Field Communication (NFC) using Radio Frequency Identity (RFID) tags have also been evolving. Convergence of these two technologies, i.e. the Internet and Sensor Networks, is leading to new possibilities and visions. The possibility of a framework that would allow direct machine-to- machine communication over the Internet has led researchers to envision the benefits of bringing more machines online and allowing them to participate in the web as a vast network of autonomous, self-organizing devices. This vision has produced a paradigm being referred to as the Internet of Things (IoT).

The Internet of Things (IoT) as being embedded in the 'Industrial Internet' (Evans and Annunziata [1]) is a new paradigm shift that comprehensively affects computers and networking technology. This is also recently referred to with the buzzword 'Industrie 4.0'. This technology is going to increase the utilization followed by Bandwidth of the Internet. More and more (intelligent) devices in this network are connected to the Internet through various combinations of sensor networks. For example, RFID tags, NFC and Bluetooth devices can be used to communicate in this

Internet-like network. Devices at home no matter their size, are given active or passive RFID tag, NFC chip, and devices like an air conditioner are attached to a transceiver to communicate with a local server. This local server updates the sensor output data into the Internet through the local server. The data from Internet is accessed from a desktop, mobile phone or any device that is connected to the Internet.

One of the main advantages of this kind of networking architecture involving home appliances and devices is that we can have control over our devices throughout a global reach where communication is possible. The potential arises on nearly every scale as we could imagine with smart cars (autonomous self-driving vehicles), smart planes (drones), smart homes and smart cities. IoT can be implemented in business or industrial environments based on the requirement enabled technically by machine-to-machine (M2M) communication (Alpaydin [2]).

There are many devices connected to the Internet. For example, to generate a print job we had to give all the instructions manually, but now we have printers that can be connected wirelessly through the Wi-Fi home network. The printing job can be done from anywhere and on any device such as a computer or a smartphone. In the same way, all the appliances and devices at home can be controlled remotely. It is achieved by arranging the devices and appliances in the smart home in a network and connecting them to a decision-making circuit. It is a centralized network because the decision-making circuit takes a decision on the status of the devices in the network.

In an IoT environment, the controlling and communication of devices involves much sensor networks with input and output ports.

What distinguishes IoT from traditional network technologies are two-fold: (i) the 'things' are of diverse nature such as machine parts, control units, communication devices,…, (ii) they engage into more complex communication similar and up to the level of human communication. B. Arthur [3], the Stanford economist and father of 'increasing returns mechanism' (IRM), terms this the Second Economy and exemplifies it like this:

"… if I'm driving in Los Angeles in 15 years time, likely it'll be a driverless car in a flow of traffic where my car is in a conversation with the cars around it that are in a conversation with general traffic and with my car. The second economy is creating for us --- slowly, quietly, and steadily --- a different world".

2. Background Research on Internet of Things

IoT means connecting things to the Internet, it can be an object or a device. The communication of devices on the Internet-like network can be one sided or two sided in terms of networking. We can say the communication can be a simplex kind of communication or duplex communication. The Internet has been using different types of technologies like http, www, and com (commercial); the communication between the devices has evolved as Internet technologies were developed. The new web development on the web are Web 2 and Web 3 technologies. In these technologies, engineers are designing the web server so that the machine can understand the instructions directly given by the user. This kind of technology will help the wireless sensor devices to communicate with the web directly, making them decision-making circuits (when given with a proper algorithm to make a decision and act accordingly).

For instance, consider an active RFID chip equipped with a relevant sensor; this RFID label usually gathers digital output from the powered sensor in the chip and sends that data to the server but does not take any action. However, when we give commands in computer language, the machine can understand the result due to which it can choose an appropriate action from the given set of actions. In this case, we are talking about machine-to-machine (M2M) communication where the machine communicates within themselves and performs an appropriate action.

Industrial driving forces in the IoT context

According to IoT development, IoT business evolves through several stages from expediting logistics to tele-operation and tele-presence as a result of the interaction forces of both market pull and technology push (Gottinger [4]). This development roadmap indicates that the progress in relevant technology will continuously contribute to the development of IoT, while the commercialization in the market place is another key issue relating to the progress of IoT. Therefore, IoT business is promoted by industrial driving forces of both technology push and market pull. First, technology push is viewed as a new invention being pushed through the development of related technologies. Rapid development of IoT technology brings enormous potential to firms in IoT business. For example, many important technologies such as cloud computing, RFID technology, and sensor network technology have promoted the development of IoT business to a new level (Whitmore et al. [5]).

Second, market pull is defined as an innovative force being developed by firms in response to an identified and/ or potential market need conditional on a given acceptable security level. Enormous market demand in IoT business provides unprecedented market opportunities to firms. For example, IoT applications in home appliances, healthcare, and automobiles are pulled by new market demands like household demand for home automation, patient demand for customized service, and customer demand for intelligent vehicles.

The International Telecommunication Union (ITU) for instance defines the Internet of Things as ''a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies'' (ITU [6])). At the same time, a multitude of alternative definitions has been proposed. Some of these definitions exhibit the connectivity scale on

the things which become connected in the IoT. Other definitions focus on Internet-related aspects of the IoT, such as Internet protocols and network technology. And a third type centers on semantic challenges in the IoT relating to the storage, search and organization of large volumes of information (Atzori et al. [7]).

While there is no universal definition for the IoT, the core concept is that everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to achieve some useful objective. The core single concepts underlying the IoT are not new. For years, technologies such as

RFID and sensor networks have been used in industrial and manufacturing contexts for tracking large-ticket items such as cranes and livestock. The idea of direct machine-to-machine communication is also not that new, as it is basic to the idea of the Internet in which clients, servers and routers communicate with each other. What the IoT represents is an evolution of the use of these existing technologies in terms of the number and kinds of devices as well as the interconnection of networks of these devices across the Internet. For example, most devices currently on the Internet were originally designed to be part of the Internet and have integrated processing, storage and network capabilities. These devices include servers, desktops laptops, tablets and smart phones. What the IoT proposes is to attach technology to everyday devices, such as audio/video receivers, smoke detectors, home appliances, etc. and making them online, even if they were not initially designed with this capability in mind. The other major evolutionary change promised by the IoT, is the integration of networks that contain these devices, making each device directly accessible through the Internet. For example, RFID has been used for years to track products through certain parts of the supply chain. However, once the product left the shelf of a retail outlet, the manufacturer 's ability to track the object was lost.

Likewise, consumers were unable to gain access to the lifecycle information of products they purchased. By giving each product a unique identifier and making its data available through the web, the IoT promises to enable product traceability throughout the entire product lifecycle.

The emerging wirelessly sensory technologies have significantly extended the sensory capabilities of devices and therefore the original concept of IoT, hence is extending to ambient intelligence and autonomous control. To date, a number of technologies are involved in IoT, such as wireless sensor networks (WSNs), barcodes, intelligent sensing, RFID, NFC, low energy wireless communications, cloud computing network depending on the standardization.

Depending on various technologies for the implementation, the definition of the IoT varies. However, the fundamental of IoT implies that objects in an IoT can be identified uniquely in the virtual representations. Within an IoT, all things are able to exchange data and if needed, process data according to predefined schemes.

3. Specific Technologies and Usage

At the core of the idea of the Internet of Things is the notion that everyday 'things' such as vehicles, refrigerators, medical equipment, and general consumer goods will be equipped with tracking and sensing capabilities. When this vision is fully actualized, 'things' will also contain more sophisticated processing and networking capabilities that will enable these smart objects to understand their environments, interact with people and become smart. Like any information system, the IoT will rely on a combination of hardware, software and architectures, and through software more and more Artificial Intelligence (AI) is being built in that makes the 'things' to act autonomous and serve as intelligent decision-making agents. (In the recent 2017 CeBIT Fair, Hannover, IBM displayed a BMW in which an AI engineered IBM Watson IoT was embedded for autonomous driving). Other industrial service examples abound under the rubric of IBM initiated 'cognitive computing' (Fingar [8]).

Some of the hardware upon which the IoT is being built already exists and is currently in industrial use. Critical hardware infrastructure includes: RFID, NFC and Sensor Networks.

Radio-Frequency Identification (RFID) is a short range communication technology where an RFID tag communicates with an RFID reader via radio-frequency electromagnetic fields. Tags may contain different forms of data, but the data form most commonly used for IoT applications is the Electronic Product Code (EPC). An EPC is a universally unique identifier for an object. These unique identifiers ensure that NFC objects tracked with RFID tags have individual identities in the IoT.

RFID is not a new technology designed specifically for the IoT. RFID's usefulness in terms of tracking objects has been well established. The technology has applications in the areas of logistics and supply chain management, aviation, food safety, retailing, public utilities and others. The use of RFID has been mandated by organizations such as Wal-Mart, the U.S. Department of Defense, and others. However, the tracking capabilities offered by RFID are generally understood to be a precursor to the Internet of Things (Ngai et al. [9]) and the benefits of RFID can be extended by making their data.

A newer technology that builds on the RFID standard is Near Field Communication (NFC). NFC is a short-range communication standard where devices are able to engage in radio communication with one another when touched together or brought into close proximity to one another. Each NFC tag contains a Unique Identification (UID) that is associated with the tag. The NFC technology is frequently integrated into smartphones which are able to exchange data with one another when brought together. NFC devices are also able to make connections with passive, unpowered NFC tags that are attached to objects. One common use for NFC is in smart posters. Smart posters contain readable NFC tags that transmit data to the user 's smart phone which reads the data from the tag.

Sensor networks are devices that monitor characteristics of the environment or other objects such as temperature, humidity, movement, and quantity. When multiple sensors are used together and interact, they are referred to as a wireless sensor network (WSN). Wireless sensor networks contain the sensors themselves and may also contain gateways that collect data from the sensors and pass it on to a server.

While sensors 'sense' the state of an environment or object, actuators perform actions to affect the environment or object in some way. Actuators can affect the environment by emitting sound, light, radio waves or even smells. These capabilities are one way that IoT objects can communicate with people. Actuators are frequently used in combination with sensors to produce sensor-actuator networks. One example of the use of actuators in such a network would be the use of a sensor to detect the presence of carbon monoxide in a room and the use of an actuator to produce a loud noise alerting people to the detection of the harmful gas. Thus, the combination of sensors and actuators can enable objects to simultaneously be aware of their environment and interact with people, both goals of the IoT.

In practical industrial usage pattern IoT presently embraces RFID-enabled identification and tracking technologies. The RFID system has been widely applied in logistics, such as package tracking, supply chain management, healthcare, monitoring and maintenance applications.

A RFID system could provide sufficient real-time information about things in IoT, which are very useful to manufacturers, distributors, and retailers. For example, RFID application in supply chain management can improve inventory management. Some identified advantages include reduced labor cost, simplified business processes, and improved efficiency.

Five years ago, it was reported that 3 percent of EU based companies are using RFID (Kranenburg and Anzelmo [10]) but with a strong growth potential. In RFID-based applications, 56 percent of firms go for access control, 29 percent for supply chain, 25 percent for freeway tolls, 24 percent for security control, 21 percent for product control, and 15 percent for asset management.

Hardware devices involve very diversified specifications in terms of communication, computation, memory, and data storage capacity, or transmission capacities. An IoT application consists of many types of devices. All types of hardware devices should be well organized through the network and be accessible via available communication. Typically, devices can be organized by gateways for the communication purpose over the Internet.

IoT can be an aggregation of heterogeneous networks, such as WSNs, wireless mesh networks, mobile networks, and Wireless Locally Area Network (WLAN). These networks help the things in fulfilling complex activities such as decision-making, computation, and data exchange. In addition, the reliable communication between gateway and things is essential to make a centralized decision with respect to IoT. The gateway is capable of running the complicate optimization algorithm locally by exploiting its network knowledge. The computational complexity is shifted from things to the gateway; the global optimal route and parameter values for the gateway can be obtained. This is feasible since the size of the gateway domain is in the order of a few of tens in comparison with the sizes of things.

Hardware capabilities and the communication requirements vary from one device type to another. The things in IoT can have very different capabilities for computation, memory, power, or communication. For instance, a cellular phone or a tablet has much better communication and computation capabilities than a special-purpose electronic product such as a heart rate monitor watch. Similarly, things can have very different requirements of Quality of Service (QoS), in particular, in the aspects of delay, energy consumption, and reliability. For example, minimizing the energy use for communication/computation purposes is a major constraint for the battery-powered devices without efficient energy harvesting techniques; this energy constraint is not critical for the devices with power supply connection.

4. Breadth of Application Areas

IoT is an interconnected network of smart objects and devices. Objects in the world of the Internet of Things, mostly referred to as smart objects, are augmented to have RFIDs, NFCs, microprocessors or sensors built in or attached to them. Networked objects create a continuous data stream, which can be connected to offer services to users. The Internet of Things affects everyday lives of people all around us. Users get information from objects, and have novel ways of interacting with them. One can swipe (or wave) a smart card to process payment while taking a bus, train or subway. One crosses a bridge, and the tollbooth automatically deducts money from the owners account. One can look at an object (e.g. with Google Goggles or with augmented reality), and one can find out all that he wants to know about the object. RFIDs are used in stores for supply chain management. Parking meters update their status, so that drivers can know the vacancy in a parking lot. Smart meters in homes give updated information about electricity consumption; smart devices communicate with the appliance to find out its electricity consumption. Shoes with embedded accelerometers keep track of the pace and distance covered while running. Bio sensors and wearable medical gadgets keep a record of the health conditions and parameters in a body.

The Internet of Things semantically means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" (Greengard [11]). This implies a huge number of (heterogeneous) objects involved in the process. The vision is a new era of data production where "humans may become the minority as generators and receivers of traffic and will be dwarfed by

those prompted by the networking of everyday objects" (ITU [6]).

The IoT is a convergence of various visions, evolving together based on the stakeholders' focus of development. Atzori et al. [7] identifies three classes of visions within the research community of the IoT: Things-oriented, Internet-oriented and Semantic-oriented. The Things oriented vision focuses on the Things in the Internet of Things. Perspectives include Near Field Communications (NFC), Wireless Sensor and Actuator Networks (WSAN), microprocessors, embedded systems, 3D and barcodes together with RFID. The Internet oriented vision is concerned with the protocols for communication networks. Some protocols are the Internet Protocol, IPv6 and the Web of Things paradigm. The third vision within the IoT is semantic oriented. The semantic oriented vision focuses on the organization, storage, retrieval, representation, interconnection, and search of the immense data coming in from interconnected objects (Toma et al. [12]). The objects are not necessarily addressed not by their unique identifiers, but by associating meaning (semantics) to their addressing and identification mechanisms.

The domain of the application areas for the IoT is limited only by imagination at this point. For a thorough discussion of the common application areas see (Atzori et al. [7]; Miorandi et al. [13]) Based on a broad review of literature, the applications categories can be sub-classified into the following application domains: smart infrastructure, healthcare, supply chains/ logistics, and social applications.

Smart infrastructure

Integrating smart objects into physical infrastructure can improve flexibility, reliability and efficiency in infrastructure operation. These benefits can reduce cost and manpower requirements as well as enhance safety.

A fully designed and implemented smart (electric) grid (SG) would be a scaled-up IoT with a big data (BD) dimension in cloud computing (CC) subject to security challenges. A SG would not only cover cost-effective and efficient cloud but also secure services applying techniques of data analytics (Li and Liu [14]). IoT technologies are also being used inside homes, offices and cities. Homes and buildings are being equipped with sensors and actuators that track utility consumption, monitor and control building infrastructure such as lights, and conduct surveillance to meet security needs (see Appendix).

On a broader scale, IoT technologies can be employed to make cities more efficient. The goal of smart cities is to leverage the IoT to improve the lives of citizens by improving traffic control, monitoring the availability of parking spaces, evaluating air quality and even providing notification when trash containers are full (Schaffers et al. [15]; Vicini et al. [16]).

Healthcare

IoT is proposed to improve the quality of human life by automating some of the basic tasks that humans must perform. In that sense, monitoring and decision making can be moved from the human side to the machine side. One of the main applications of IoT in healthcare is in assisted living scenarios. Sensors can be placed on health monitoring equipment used by patients. The information collected by these sensors is made available on the Internet to doctors, family members and other interested parties in order to improve treatment and responsiveness (Dohr et al. [17]). Additionally, IoT devices can be used to monitor a patient's current medicines and evaluate the risk of new medications in terms of allergic reactions and adverse interactions.

Supply chains/logistics

RFID and sensor networks already have long established roles in supply chains. Sensors have long been used in assembly lines in manufacturing facilities and RFID is frequently used to track products through the part of the supply chain controlled by a specific enterprise. While the use of these technologies in supply chains is not new, the pervasiveness and ubiquity ('ubiquitous computing') promised by the IoT will enable the use of these technologies across organizational and geographic boundaries. Specifically, the IoT can further improve logistics and supply chain efficiency by providing information that is more detailed and up-to-date (Flügel and Gehrmann [18]).

5. Security of Things

For IoT, security and privacy are two important challenges. To integrate the devices of sensing layers as intrinsic parts of the IoT, effective security technology is essential to ensure security and privacy protection in various activities such as personal activities, business processes, transportations, and information protection (Tan et al. [19]; Wang et al. [20]; Xing et al. [21]). The applications of IoT might be affected by pervasive threats such as RFID tags attacks and data leakage. A number of security issues could be approached beyond a basic cryptographic structure either through software tools, decentralized random control and through artificial intelligence techniques providing any component of the IoT with an inherent security control. What is essentially needed though not yet available is some universal safe-proof security design that comprises all these elements.

"The Internet wasn't designed with security in mind and, in todays world, security experts are playing a game of cat and and mouse with cybercrooks and hackers. As every new threat and breach occurs, security teams scramble to plug the dike. This has led to a mélange of tools, approaches and techniques- none of which solves the problem alone" (Greengard [11], Chap.6).

In RFID systems, a number of security schemes and authentication protocols have been proposed to cope with security threats.

Recently, in their IoT Security Architecture under 'Threat Intelligence' IBM invokes their AI based Watson program for integrated security assessment.

IoT devices are typically wireless and may be located in public places. Wireless communication in today's Internet is typically made more secure through encryption. Encryption is also seen as key to ensuring information security in the IoT. How-ever, many IoT devices are not currently powerful

enough to support robust encryption. To enable encryption on the IoT, algorithms need to be made more efficient and less energy- consuming, and efficient key distribution schemes are needed (Yan and Wen [22]).

In addition to encryption, identity management is an important component of any security model and unique identifiers are essential to IoT devices. These identifiers may be used to establish personal identities at financial institutions, identify illegal activity and other functions.

Thus, ensuring that smart objects are who they say they are is essential to IoT success (Mahalle et al. [23]; Roman et al. [24]).

Privacy

As more and more objects become traceable through IoT, threats to personal privacy become more serious. In addition to securing data to make sure that it doesn't fall into the wrong hands, issues of data ownership need to be addressed in order to ensure that users feel comfortable participating in the IoT.

Thus, the ownership of data collect ed from smart objects must be clearly established. The data owner must be assured that the data will not be used without his/her consent, particularly when the data will be shared. Privacy policies can be one approach to ensuring the privacy of information. Smart objects and reading devices in the IoT can each be equipped with privacy policies. When the object and reader come into contact, they can each check the other 's privacy policy for compatibility before communicating (Roman et al. [24]).

6. Economic Benefits

In a survey on IoT and its 'economic energy' Fleisch [25], p. 14 addresses one of the core economic impacts of IoT:

"The IOT, with its technologies to automate the bridging of the last mile between the Internet and the physical world, dissolves the transaction costs that are caused by real world-virtual world media breaks. A real world-virtual world media break occurs when a piece of information is transferred from one carrier medium, e.g., a bar code, to another, e.g., a data base that serves a warehouse management system. When things become computers, these media breaks, along with their attached costs fade away."

In specific IoT applications, the costs of interactive objects in production or service industries would not carry only physical (material) or labor costs but also coordination or regulatory costs, the costs of transaction. Depending on the industry, its scale, scope and value generation, they could be substantial and even dominate the others. Thus cost avoidance or substantial reduction would have multiple benefits for any network industry concerned, nationally and across borders. For the companies in that industry would benefit in industrial competitiveness in an international context. On the other hand, they could even reverse or at least diminish past and current flows of trade in manufactured goods from emerging to advanced economies.

This equally well applies to supply chains in industrial economies. The dynamics of relationship among supply chain partners is viewed in terms of their respective innovation competence. It is emphasized that varying power arrangements (through information asymmetry) in a supply chain leads to different implications for investments in innovation by buyer and supplier (Gottinger [26]).

Williamson's [27], [28] transaction cost approach provides a conceptual grounding for understanding the fundamental basis on which relationship between buyer and supplier takes place. With multiple firms constituting a supply chain, investments by supply chain partners have implications that transcend the traditional cost minimization or revenue/profit maximization objectives. In present dynamic environments, firms are investing in risky innovations and pursue associated strategies to gain first-mover advantage. In high technology industries more firms strategically decide to enter a collaborative relationship. In a joint product development context, many firms outsource the manufacturing process of components which would be used in the final product. At times, this outsourcing goes beyond just the manufacturing of a fully specified component to allowing and expecting the supplier to build resource competence through active innovation.

With a decrease of transaction costs through IoT we could also envision a decrease in quality of control costs through IoT induced network industries increasing the value chain of its producers lifting their productivity and their profitability and boosting industrial growth.

The GE Report on the Industrial Internet by Evans and Annunziata [1] foresees those benefits in particular, in the aviation, transportation, electric power and distribution ('smart grids'), the retail and healthcare industries facilitated through complementary enabling elements in intelligent machines, advanced data analytics and networked people at work.

Those industries in particular are bound to favor 'increasing returns mechanisms' that generally speaking complementarize technologies, business operations and strategies and form the core engine of network-centered industrial growth. (Gottinger [29], Chaps. 4, 7), and with its diverse potential IoT is bound to give rise to combinatorial innovation.

In terms of cumulative benefits, over another decade from 2014 for the 'Internet of Everything' (i.e. IoT plus intrinsic human connectivity) facilitated by the 'Smart Cities' movement the CEO of Cisco Systems John Chambers [30] points to a ballpark figure of value added to the global economy by about $ 19 Trillion (or $19 thousand billion)

On a more negative note, the IoT, in some industries, may contribute to replace jobs and even may not create new ones beyond the commonly observed process of automation. In the mid to longer term the net effects of jobs replacement may well be negative according to MIT economists Brynjolfsson and McAfee [31] but a final verdict is out there.

As with all other economic activities network externalities

could well have positive economic impacts but could well be negative as in the case of security breaches, cyber piracy and loss of privacy potentially inducing irreversible economic damages that would be even out of proportion with a universal scalable and scaling effect of IoT. As in the economics treatment of accident law this requires assessment of a delicate balance of tradeoffs and compensation.

Summarizing we can say that IoT promises multiple economic benefits such as

(1) lowering transaction costs for various industries and the entire economy, improving quality of products, services for consumers, and quality of life in environmental protection and energy provision,

(2) enabling substantial industrial performance in a broad set of value generating industries and therefore inducing industrial and economic growth and well being though without creating new jobs in some industries.

7. Future Directions

Since the IoT has not yet been fully realized – conceptually and in practical implementations, it might seem precocious to forecast the future directions, the extent of industrial broadening and deepening of IoT. Yet, the manufacturing sector together with 3D Printing and supply side chaining will be universally affected.

As regards the Industrial Internet it has been a major theme on the World Economic Forum's (WEF) 2016 Annual Meeting at Davos, also we have had a comprehensive showcase at the CEBIT and the Hannover Industrial Fair (2016, 2017) with companies such as Siemens, ABB, Intel, IBM, Huawei, ZTE, Bosch, Kuka, Fanuc, Kawasaki in partnership with software firms showing their projects, and exposing over 100 cases of real-world implementations of Industry 4.0. Future visions of the IoT will affect its current development and must therefore be considered.

One future vision for the IoT is the Web of Things. The Web of Things proposes the use of web standards to fully integrate smart objects into the World Wide Web (WWW). Using web technologies can make it easier for developers to build applications using smart objects and existing web protocols can more easily enable the interoperability and communication of different devices. A mashup is a Web 2.0 concept where an application uses data and functionality from a variety of web resources. Some researchers proposing the Web of Things model suggest building on the mashup paradigm, except this time applying it to physical devices instead of applications (Guinard et al. [32]).

With the generality of the Web, the WoT and IoT are on the edge of experiencing vast progress. Today, we are one step closer to this vision due to latest advances in web services, identification technologies, convergence services, wireless networks, which make communication capabilities and processing power available in increasingly smaller packages. Obviously, the Internet is evolving into the so-called 'Web of Things' (WoT), an environment where everyday devices such as traffic lights, sidewalks, buildings, and commodities are recognizable, identifiable, addressable, and even controllable via the Internet. Certainly, starting from an Internet of nearly one thousand million computers, the Web now turns to be an Internet of nearly 100 billion of things or devices presaging transition from an IoT to a WoT. Thus, in a WoT platform the workload is put at the extreme level and scalability is a compulsory requirement.

This does not refer to any technology or any network structure, but only to the idea of interconnecting devices as well as interconnecting computers with the Internet. Use of the Web as the platform hosting and exposing connected devices can be explained by multiple technological and economic benefits, a few of which include deployment, high availability and versatility, use of standardized communication protocols and the ecosystem created thanks to Web 2.0 paradigm. A thing or object becomes Internet-enabled if it is associated with networking ability, which peculiarly identifies it on the Internet. Recently, devices or objects such as electric meters, access cards, street lights, and sensors are already accessed and networked on to the Internet. A thing or object becomes Web-enabled when it is augmented with a Web server so that it can exploit its functional and non-functional abilities on the Web through http. Researchers have long ago successfully embedded tiny Web servers on resource-constrained things, making Web-enabled things or devices a reality. Certainly, there is a domain for Representational State Transfer (REST) in the area of Web services. The advances in REST based web service structure are the abstraction of physical things as services on the Web. This trend gives rise to the possibilities of wrapping things in the physical world as Web services.

8. Conclusions

This paper reported on the current state of IoT research by challenges that threaten IoT diffusion, presenting open research questions and future directions, and compiling a comprehensive reference list to assist researchers. We proposed a classification scheme with six major categories: technology, applications, challenges, business models, future directions and overview/survey.

The IoT holds the promise of improving people's lives through both automation and augmentation. The capabilities offered by the IoT can save people and organizations time and money as well as help improve decision making and outcomes in a wide range of application areas. The IoT builds on existing technologies such as RFID and Wireless Sensor Networks along with standards and protocols to support machine-to-machine communication such as those envisioned for the semantic web. One question that remains is whether or not the IoT is to be an enduring technology, whether it will fail to materialize universally, or whether it is only a stepping stone to another paradigm. Only time will ultimately answer that question. However, by bringing existing technologies together in a novel way, the IoT has the potential to reshape our world.

Appendix: Smart Home Skeleton Design – An Illustrative Example

A home becomes smart if the access and control of the devices and utilities in the home start taking a decision (we are not talking here about Artificial Intelligence). These devices start making the decision if a proper set of instructions is given to them, and only if Machine to machine communication is happening. Machine to machine learning is possible if sensor networks control these devices. Technologies, protocols, networks like RFID, NFC, Zigbee, Z-wave, Wi-Fi, Wi-max, Bluetooth and various sensors (temperature, PIR, smoke, and humidity) can make a decision-making circuit. The features below illustratively explain the communication process.

Smart home network.

We can see small circuits (sensors and smart circuits) fixed on all the devices and appliances, these sensors and decision-making circuits communicate with access gateway. The access gateway is connected to a local router that provides Internet connection through which the data is transferred to the Internet.

Smart homes have the following features:

1) Decision making circuits.
2) Power efficient devices.
3) Remote access.
4) Security.
5) User friendly.

1. Decision Making Circuits

Decision-making circuits are nothing but the sensors with a combination of programmable memory device and transmitter (wired or wireless) which make decisions depending on the input from the sensors. The sensor data is converted into machine understandable format and given to the memory unit that compares the predefined set of instructions and performs an appropriate action. The performed action and the status of the sensor are transmitted to the gateway so that the user can know the situation of that particular device.

2. Power Efficient Appliances

High-efficiency appliances are used to get the same output as the regular appliance but consume minimal power. Appliances like high-intensity LEDs and power saving appliances are installed to make smart utilization of energy without compromising on comfort levels.

3. Remote Access

The main purpose of smart homes is to achieve control over appliances remotely.

Most of the times we see, people forget to switch off the appliances while rushing to work due to which they have to pay higher electricity bills and frequent breakdown of appliance's due to excessive usage. The appliances, when linked to a universal controlare accessible from anywhere remotely with our smartphones and computers, the user can switch them as he/she wants and monitor their home.

4. Security

We build our home the way we want, and we also want it to stay the same way, so safety is also the primary concern in a smart home. For safety from fire water and high temperature, appropriate sensors should be installed to alert us in cases of fire breakout or water leakage. Our smart home can also be vulnerable to robbery. To prevent our house from getting robbed, we can install cameras that record the footage in the cloud. Also to get informed on any unauthorized entries and suspicious behavior, infrared alarm system (it could be a PIR sensor or burglar alarm system) can be arranged in the fencing and entrances.

5. User Friendly

All the members living in the house may not be aware of the latest technology (elderly people), so the operation of these appliances should be easily understandable for people of all age groups. A simple system is designed so that user can troubleshoot on its self. The interface of control should also be as simple and friendly as possible.

For illustrative purposes, we have designed a model to demonstrate Internet of Things for remote monitoring and controlling of appliances remotely through the Internet using a web interface. The objective of this model is to provide nonphysical control over appliances and to give an update on the temperature and humidity levels at home through the web interface from anywhere in the world. This kind of a model helps the physically challenged and the aged persons to control appliances as it might be difficult for them to move to the switch every time they want to control it. Moreover, the proposed model is cost effective and power efficient.

The concept of Internet of Things can be further improved by creating a proper interface and designing a specific user-friendly gateway to communicate with the Internet. Available goods and quantity can be known in a single scan when all the objects and goods are given an RFID tag. In a similar way misplaced lost and found objects can be tracked using this concept by tracking them using appropriate sensors fixed to them. A mobile application can be created to control these appliances from our smart phones. By arranging cameras in business places, every camera can be operated and monitored from anywhere by logging into the account. Similarly, this technology can be implemented in various applications for easy accessibility.

References

[1] Evans, P. C. and Annunziata, M. (2012). Industrial Internet, General Electric (GE) Report, New York.

[2] Alpaydin, E. (2016). Machine Learning, The New AI, Cambridge, Ma.: MIT Press.

[3] Arthur, B. (2011), "The Second Economy", McKinsey Quarterly, Oct.

[4] Gottinger, H. W. (2006). Innovation, Technology and Hypercompetition, London: Routledge.

[5] Whitmore, A., Agarwal, A. and Da Xu, L. (2015). "The Internet of Things—A survey of topics and trends ", Inf Syst Front 17, 261–274.

[6] ITU (2013). The Internet of Things, International Telecommunication Union (ITU), Internet Report [2013, May 20]; available from http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-I R.IT-2005-SUM-PDF-E.pdf.

[7] Atzori, L., Iera, A. and Morabito, G. (2010). "The Internet of Things: A survey", Computer Networks, 54(15), 2787–2805.

[8] Fingar, P. (2015). Cognitive Computing, Tampa, Fl.: Meghan-Kiffer Press.

[9] Ngai, E. et al (2008)." RFID research: an academic literature. review (1995–2005) and future research directions", International Journal of Production Economics 112(2), 510–520.

[10] Kranenburg, R. and Anzelmo, E. (2011)."The Internet of Things", 1st Berlin Symposium on Internet and Society, Oct 25–27, in Inf Syst Front. 17, 2015, 243–259.

[11] Greengard, C. (2015). The Internet of Things, Cambridge, Ma: MIT Press.

[12] Toma, I., Simperl, E. and Hench, G. (2009). "A joint roadmap for Semantic technologies and the Internet of Things", Technology, 1–5.

[13] Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012)."Internet of things: vision, applications and research challenges.", Ad hoc Networks, 10 (7), 1497–1516.

[14] Li, L., and Liu, J. (2012). "An efficient and flexible web services-based multidisciplinary design optimisation framework for complex engi- neering systems", Enterprise Information Systems, 6(3), 345–371.

[15] Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., and Oliveira, A. (2011)." Smart cities and the future internet: Towards cooperation frameworks for open innovation", in Domingue, J. et al. Eds. (2011). The future Internet, Lecture Notes in Computer Science (Vol. 6656), 431–446, Berlin: Springer.

[16] Vicini, S., Sanna, A. and Bellini, S. (2012). "A living lab for Internet of Things vending machines", in Uckelmann, D., Scholz-Reiter, B., Rügge, I., Hong, B. and Rizzi, A., Eds. (2012). The Impact of Virtual, Remote, and real Logistics Labs, Communications in Computer and Information Science 282, 35–43, Berlin: Springer.

[17] Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., and Schreier, G. (2010). "The Internet of Things for ambient assisted living", Proceedings of the Seventh International Conference on Information Technology: New Generations (ITNG).

[18] Flügel, C., and Gehrmann, V. (2009). "Scientific Workshop 4: Intelligent objects for the Internet of Things: Internet of Things – application of sensor networks in logistics", in Gerhäuser, H., Hupp, J, Efstratiou, C., and Heppner, J., Eds. (2009). Constructing ambient intelligence, communi- cations in computer and information science (Vol. 32), 16–26. Berlin: Springer.

[19] Tan, L., and Wang, N. (2010). "Future Internet: The Internet of Things", Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).

[20] Wang, S., Li, L., Wang, K., and Jones, J. D. (2012). "e-Business systems integration: a systems perspective", Information Technology and Management, 13 (4), 233–249.

[21] Xing, Y., Li, L., Bi, Z., Wilamowska-Korsak, M., and L. Zhang, L. (2013). "Operations research (OR) in service industries: a comprehensive review", Systems Research and Behavioral Science, 30 (3), 300–353.

[22] Yan, T. and Wen, Q. (2011). "Building the Internet of Things using a mobile RFID security protocol based on information technol- ogy", Adv. Comput. Sci. Intell. Syst. Environ. 104, 143–149.

[23] Mahalle, P., Babar, S., Prasad, N. R. and Prasad, R. (2010)."Identity management framework towards Internet of Things (IoT): Roadmap and key challenges", in Meghanathan, N. et al. Eds. (2010). Recent trends in network security and applications, communications in computer and information science (Vol. 89), 430–439, Berlin: Springer.

[24] Roman, R., Najera, P. and Lopez, J. (2011)."Securing the Internet of Things", IEEE Computers, 44(9), 51–58.

[25] Fleisch, E. (2013). "What is the Internet of things?" [cited 2013, May 20]; available from http: / / www. im. Ethz. ch / education / HS10 / AUTOIDLABS-WP-BIZAPP-53.pdf.

[26] Gottinger, H. W. (2015). "Supply-Chain Coopetition", International Journal of Business and Economics Research 4(2), 67-71 (www.sciencepublishinggroup.com/j/ijber).

[27] Williamson, O. E. Ed. (1995). Organization Theory, New York: Oxford Univ. Press.

[28] Williamson, O. E. (1996). The Mechanisms of Governance, New York: Oxford Univ. Press.

[29] Gottinger, H. W. (2016). Networks, Competition, Innovation and Industrial Growth, New York: Nova Science.

[30] Chambers, J. and Elfrink, W. (2014) "The Future of Cities. The internet of Everything will change how we live", in Special Issue of Foreign Affairs 2016, G. Rose, editor.

[31] Brynjolfsson and McAfee, A. (2011). The Race against the Machine, Lexington, Ma.: Digital Frontier Press.

[32] Guinard, D., Trifa, V., Mattern, F., and Wilde, E. (2011). "From the Internet of Things to the Web of Things: Resource-oriented architecture and best Practices", in Uckelmann, D., Harrison, M. and Michahelles, F., Eds. (2010). Architecting the Internet of Things, 97–129, Berlin: Springer.