Journal of Social Sciences *Vol. IV, no. 2 (2021), pp. 107 - 116*
Fascicle *Social Science* *ISSN 2587-3490*
Topic *Marketing and Logistics* *eISSN 2587-3504*

https://doi.org/10.52326/jss.utm.2021.4(2).11
UDC 004.7:621.391

INTERNET OF THINGS (IOT) CONQUERS THE WHOLE GLOBE

Titu-Marius I. Băjenescu*, ORCID ID: 0000-0002-9371-6766

Swiss Technology Association, Electronics Group Switzerland
**tmbajenesco@gmail.com*

Received: 04.28.2021
Accepted: 05.22.2021

Abstract. The article examines the market for connected objects, which is gradually taking its place in the global economy**.** Autonomous cars, smartphones, video surveillance, connected objects are already present in our daily lives. However, it is in industry that the Internet of Things has developed the most. The Internet of Things, or IoT**,** is a concept defining the extension of the Internet to physical objects. This includes not only the connected objects, but also the sensors, software and network through which these objects operate. All connected objects are powered by software, which collects data - that are then processed in the cloud. They are, therefore, programmed and programmable objects that can interact via a WiFi, Bluetooth or 4G connection. Connected objects can be found in two main applications: an industrial application and an everyday application. In the industrial sector, connected objects are very well established in various sectors of activity: automotive, aeronautics, agriculture, health, commerce, public sector, logistics, etc. Everyday applications, known as consumer applications, are struggling to develop despite the announced Eldorado. Even though many connected everyday objects exist (toothbrushes, hoovers, watches, home automation, etc.), the business model is having trouble being set up and connected objects are having trouble proving their usefulness in everyday life. There needs to be consistency and logic in the range of connected products on offer and not just a range of independent products.

Keywords: *ATM, streaming video, file sharing, online shopping, banking, social networking, toothbrushes, hoovers, watches, home automation, social impact, medical applications.*

Rezumat. În articol este examinată piața obiectelor conectate, care își ia treptat locul în economia globală. Mașinile autonome, smartphone-urile, supravegherea video, obiectele conectate sunt deja prezente în viața noastră de zi cu zi. Cu toate acestea, Internetul obiectelor s-a dezvoltat cel mai mult în industrie. Internetul obiectelor, sau IoT, este un concept care definește extinderea internetului la obiectele fizice. Aceasta include nu numai obiectele conectate, ci și senzorii, software-ul și rețeaua prin care acționează aceste obiecte. Toate obiectele conectate sunt alimentate de software, care colectează date - care sunt apoi procesate în cloud. Prin urmare, acestea sunt obiecte programate și programabile care pot interacționa printr-o conexiune WiFi, Bluetooth sau 4G. Obiectele conectate pot fi

găsite în două aplicații principale: o aplicație industrială și o aplicație de zi cu zi. În sectorul industrial, obiectele conectate sunt foarte bine stabilite în diverse sectoare de activitate: auto, aeronautică, agricultură, sănătate, comerț, sector public, logistică etc. Aplicațiile zilnice, cunoscute sub numele de aplicații pentru consumatori, se luptă să se dezvolte în ciuda anunțului Eldorado. Chiar dacă există multe obiecte de zi cu zi conectate (periuțe de dinți, hoover-uri, ceasuri, sisteme de automatizare a casei etc.), modelul de afaceri are probleme în a fi configurat, iar obiectele conectate au probleme în a-și demonstra utilitatea în viața de zi cu zi. Trebuie să existe coerență și logică în gama de produse conectate oferite și nu doar o gamă de produse independente.

Cuvinte cheie: *bancomat, streaming video, partajare de fișiere, cumpărături online, activități bancare, rețele sociale, periuțe de dinți, hoover-uri, ceasuri, automatizări casnice, impact social, aplicații medicale.*

Introduction

In early 1926, Nikola Tesla imagined a "connected world". He told *Colliers Magazine* in an interview, "When the wireless application is perfectly applied, the whole Earth will be transformed into a huge brain (while all objects constitute the real world), and the instrument by which we will be able to do this will be amazingly simple - compared to our present telephone. A man will be able to carry it in his vest pocket."

The term *IoT* - first proposed in 1999 by Englishman Kevin Ashton - has the potential to influence everything (from new production opportunities to optimizing a shop floor, from remote monitoring of worker efficiency to controlling physical assets and productivity) thanks to applications as diverse as home security and monitoring the state of a factory (Figure 1).

Figure 1. The Internet of Things.

In the same year, Gershenfeld published the paper "When Things Start to think," in which "things start to use the Net". ATMs (*Automated Teller Machines*) could be considered the first intelligent objects to come online as early as 1974.

Gradually, machines are becoming more and more digitized and connected - establishing networks between machines, people and the Internet - leading to new ecosystems that enable higher productivity, better energy efficiency, and higher profitability. Sensors enable recognition of the state of objects, with the advantage of being

able to predict people's needs based on information gathered through context. These devices cannot only gather information from their environment, but are able to make decisions without human intervention. IoT technology is used in our everyday lives; she allows the opening of a door without having a key, automatic recognition of credit cards, automatic opening of door locks, reaching vehicle detection systems, toll payment systems on highways; IoT technology is used for animal tracking and tracing, access control, payment systems using *contact-less* chip cards, anti-theft devices, etc. The building blocks of IoT are built on devices that allow them to be networked; they provide common platforms that allow them to communicate with each other, developing new applications to conquer new users [1].

The Internet is now widely used by more than a billion people for a multitude of services: searching for information, streaming video, file sharing, online shopping, banking, social networking, etc [2]. While the Internet continues to evolve, it will not only be able to allow people to communicate with each other or with a service; it will also allow objects to connect to each other to obtain and share information or to take an action. This is commonly referred to as the Internet of Things IoT and it provides the basis for the next Internet and Web 3.0 (Figure 2). As the potential number of devices that could be connected to the Internet grows, the volume of traffic generated explodes; it will be necessary to reconsider the protocols that will support the IoT**.** Most IoT projects are motivated by the need to reduce costs or increase revenue.

Translated as closely as possible to the meaning of the words, the Internet of Things is nothing more than networking objects, connecting them. An object can be a car, a toothbrush, a wristwatch, a TV, etc.

IoT is starting to take over entire sectors - such as healthcare, transport, agriculture and even industry. Studies have shown that thanks to IoT - the third wave of the Internet - by 2020, more than 26 billion objects will be connected, representing a market worth more than $300 billion.

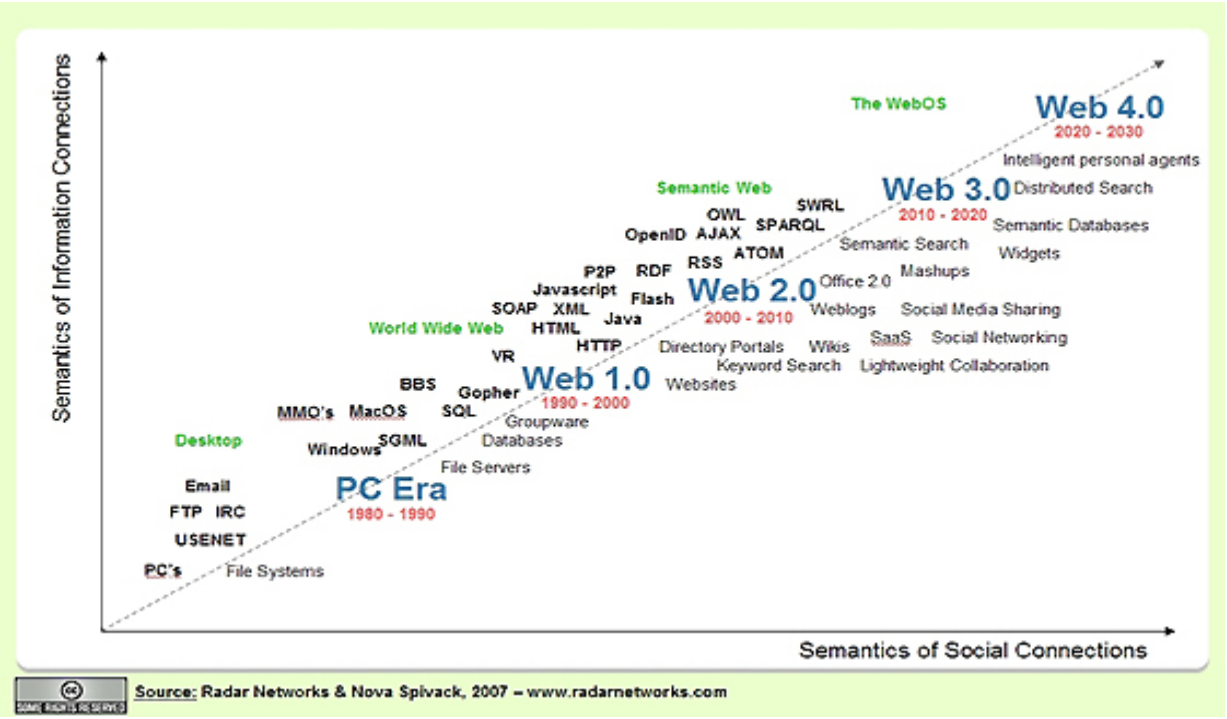

Figure 2. The Internet of Things provides the basis for the next Internet and Web 3.0.

According to the *BI Intelligence* report, IoT will be the world's largest market for electronic devices. In 2019, the number of connected computers, touch tablets and cars doubled compared to 2018. This explains why most companies have created special departments or cells dedicated to IoT, from IT service companies to large industrial groups [3]. IoT is a typical example of big data. For viable solutions, artificial intelligence (AI) techniques are considered the best choice. Therefore, IoT combined with AI techniques is the best choice; it allows us to have smart applications - such as smart e-health, smart metering and smart city. Although IoT is on everyone's mind today, security issues must be at the forefront to prevent an intruder from causing disastrous consequences.

IoT is a world of interconnected objects capable of perceiving, acting and communicating with each other and with the environment (in other words: smart things or objects) while providing the ability to share/share information and to act, in part, autonomously from real/physical world events, triggering processes and creating services with or without direct human intervention [4].

Kevin Ashton was the first to use the term *Internet of Things* (IoT) in 1999, in the context of supply chain management with radio frequency identifiers (RFID) that provide greater business efficiency and accountability.

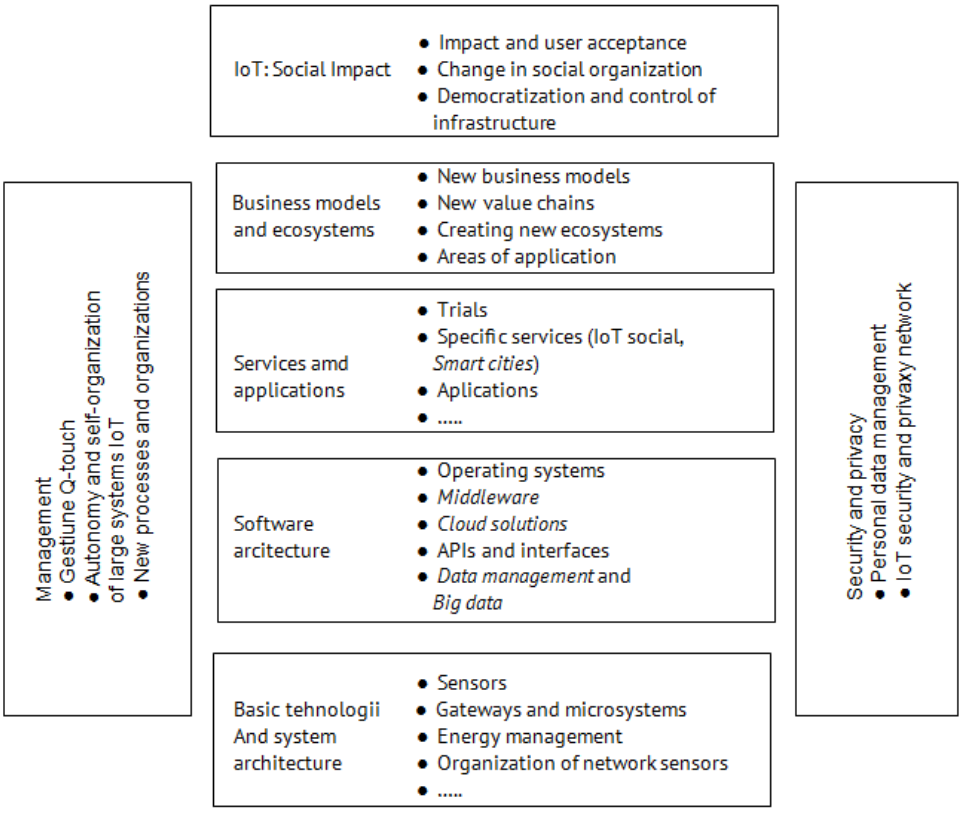

Figure 3. Technological and social aspects of IoT.

Some definitions

Since IoT is constantly evolving - and its definition continues to evolve. Accordingly, the IEEE IoT initiative provides an opportunity for members of the international community to help define IoT (*IEEE, 2015, 2017*). The document presents two definitions, one for small-scale scenarios: "An IoT is a network that connects uniquely identifiable objects over the Internet. The objects have sensing/actuation and potential programmability capabilities."

By exploiting a unique identification and a unique meaning, information about the "object" can be gathered and the state of "things" can be changed from anywhere, anytime, by anyone. The second definition is for large-scale scenarios: "IoT envisages a self-configuring, complex and adaptive network that interconnects "things" with the Internet using standard communication protocols. The interconnected objects have a physical or virtual representation in the digital world, a sensing capability, an actuation capability, a programmable feature and can be uniquely identified. The representation contains information including object identity, status, location or any other relevant commercial, social or private information [5]. Objects provide services, with or without human intervention, by exploiting unique identification, data capture and communication, and actuation capability. The service is operated through the use of intelligent interfaces, is available anywhere, anytime and for anything, taking into account security.

As technology advances, our interaction with computer systems is changing, both at work and at leisure. Information, sensor and network technology is becoming more powerful and more frequently used. People are no longer confronted with information technology only at the common points of their lives - such as at home or in the office - but also in information and communication infrastructures, present in increasingly important areas of everyday life. These infrastructures are characterized by the fact that they include not only traditional devices - e.g. PCs and mobile phones; information and communication technology is also embedded in objects and environments.

By physically embedding *IoT,* everyday objects and our everyday environment become 'smart', i.e. able to process and deliver information, but not necessarily smart in the sense of human cognitive intelligence.

Genezis of IoT

In many people's minds, the Internet of Things is a revolutionary concept. Ask an embedded/embedded systems engineer the question and they will tell you that IoT is just a natural evolution. Embedded electronic systems have been around for a long time, most of them autonomous. The ability of these embedded systems to communicate with other systems gave birth to IoT. Indeed, before the democratization of IoT, machines could already communicate with each other, and exchange information, using protocols such as RS232, RS484, etc. Broadening the modes of communication with the TCP/IP protocol, machines can now communicate over the Internet - giving rise to the IoT**.** Simply put, the IoT is nothing more than an electronic system that has the ability to exchange data with other electronic systems using TCP/IP. There are other ways of communicating today - such as radio or GSM technologies.

Basic concepts

A smart object is a physical object in which a processor, a data storage system, a sensor system and network technology are embedded. Some smart objects can also affect the environment through actuators. In principle, all physical objects can be turned into smart objects, for example ordinary everyday objects such as pens, wristwatches (there are many models of wristwatches with sensors and processors, e.g. to measure heart rate or determine geographical location) or cars (more recently autonomous cars). In an industrial context, it can be a machine or a product to be handled. Smart objects can also be anywhere. In fact, there are almost no restrictions in terms of domains: consumer electronics, household appliances, medical devices, cameras and all sorts of sensors and

data-generating devices [6]. Most smart objects have a user interface and interaction capabilities to communicate with the environment or other devices (e.g. displays). The ability of smart objects to communicate with other objects and their environment is a central component of the Internet. In summary, the idea is that specific information can be retrieved via any networked smart object, which is identified and located, and can have its own, "home page" i.e. a unique address.

Today we can take advantage of a wide range of cheap, tiny and relatively powerful components, including sensors, actuators and single board computers (SBCs), to enrich physical objects and connect them to the Internet. SBCs such as Raspberry Pi, BeagleBone Black and Intel Edison Open, as well as open source electronics such as Arduino - which entered the market between 2005 and 2008 - have catalysed millions of new ideas and projects. Creating and collecting data about the state of physical objects can form the basis of exciting home and office automation, education and leisure activities, with real-time visualisation of information generated by data 'on the move'. Moreover, remote networks of smart devices, deployed elsewhere, at another location, can be used. Closely related to 'smart objects' is the concept of 'smart environments'. One definition emphasises the extent to which smart objects are deployed and interact. A compilation of smart objects in a given space, such as an enclosed space (car, house, room) or an outdoor space - such as a district or an entire city (a smart city) transforms an ordinary environment into a smart environment. Another definition says that sensors are the key factor of a smart environment [7]. Essential to a smart environment is the contextual information gathered by sensors to provide tailored applications and services. We can define a smart environment as the physical world - which is richly and invisibly interwoven with sensors, actuators, displays and computing elements - the environment being seamlessly integrated into the everyday objects of our daily lives, connected by a continuous network.

The need for qualified staff

The tremendous growth of IoT will need a skilled workforce. Positions for IoT engineers or connected object engineers are already starting to emerge. These IoT engineers are very good technicians who master both the hardware and the application side of embedded systems. Embedded systems and information systems engineers will be the orchestra leaders of this digital revolution. Indeed, these experts will be responsible for designing and programming sophisticated electronic systems that allow our objects to communicate. On the software side, computer engineers specializing in information systems will design the infrastructures needed to collect, process, store and analyze data. When you say data, you also say information systems and security issues. This will involve the expertise of engineers specializing in data security and protection.

Some areas of IoT applications

For continuous visual tracking of passengers travelling in a vehicle, the transmission of visual light transmission (VLT) and visual light transmission (VRT visual light reflectance***)*** of the glass windows used in the vehicle should be at a certain value.

All vehicle manufacturers comply with certain standards; however, the vehicle owner/user generally buys tinted films on the gray market - and sticks them on the glass windows - which obstructs visibility and does not allow law enforcement authorities to have a clear view of who is riding in the vehicle.

The *Social Internet of things* (SIoT) is an emerging topic of the digital age with social, economic and technical significance. IoT has already proven its dominance in a wide range of sectors such as consumer products, durable goods, transport, industrial and utility components, sensors [8]. Now it is extending to social environments. The evolution of the powerful navigational capabilities of social networks is transforming social life into a new era of link prediction, community grouping, recommended systems, sentiment analysis and more. *Biometrics studies*. It has been established that a typical common pattern is a behavioral biometric trait in biometric science related to user identification/authentication system issues. However, the model being cost-effective and non-intrusive, its dynamics are a strong alternative to other biometric modalities. The model can be easily integrated into any existing knowledge-based user authentication system with minor alternations. The accuracy achieved in previous studies is impressive, but not acceptable in practice due to intra-class variation issues or data acquisition techniques.

Nanotechnology is playing an important role in changing the world by developing new technologies in areas such as healthcare, manufacturing, agriculture and industrial control systems [9]. The recent development of the *internet of nano-objects* (IoNT) is contributing to the production of new nano devices. Most of the devices we use today are equipped with sensors that have the ability to communicate and acquire intelligence. *Ambient assisted living* (AAL) has attracted the attention of dependent elderly people who are in care. AAL systems are IoT systems designed exclusively to assist older people in their daily activities. Developing a software model in AAL will enhance the functionality of the system, which is essential in managing emergency situations faced by older people.

How do IoT objects communicate? IoT is a system of interconnected computing devices, mechanical and digital machines and appliances, objects, animals or people that have unique identifiers and the ability to transfer data over a network without the need for human-computer interaction. We will need to know how devices or objects in the IoT communicate and how the meaningful names will translate the name service in the machine into an understandable form. To do this we will need to know how naming services are changed in the IoT, how their *naming, addressing, and profile server* (NAPS) overcomes these challenges [10].

Medical applications. In general, an IoT application focuses on timely service and improves efficiency. For this reason, many IoT-based healthcare devices have been developed to provide appropriate treatment to patients in a timely manner. In healthcare, such devices have adopted the principle of easy communication protocols between different IoT-based healthcare services. Recent technologies have been introduced to mitigate security issues in IoT healthcare - by adopting different security protocols and standards and focusing on detailed studies of security issues in communication between devices - through step-by-step implementation of Contiki network simulator.

Security issues in many IoT deployments, while presenting in the information technology domain, offer a lot of unique challenges. It is a fundamental priority to address these challenges to prove that IoT products and services are secures. IoT devices are vulnerable to attack because the systems have a very low-level of protection and security. That is why innovative frameworks propose the development of a secure system along with authentication. The collaborative, learning approach has proven to be an ideal model to recognize the intruder pattern, and the system can provide a solution based on this model.

Epidemiological triad. Diseases occur due to the interaction of the agent, the host and the environment, the so-called 'epidemiological triad'. There are many reasons for the failure to prevent disease complications. Due to lack of experience and time, doctors only address the bio-medical side of the disease and ignore the other important aspects. The science of disease and the art of healing by physicians must be incorporated into computational carrier services. Electronic maintenance of health records is done by connecting IoT devices to the system so that the doctor can view the data on the table. IoT is a boon to the medical field because it saves doctors time handling other calls. Wearable devices, such as those that record children's fevers, reduce the risk of illness by regularly monitoring sensor data. Using IoT puts health in the hands of patients.

Inter-operable. Billions of devices will be connected to the Internet in the near future. This will ensure inter-operable between IoT elements - one of the most important requirements to support the targeting, tracking and discovery of objects as well as the representation, storage and exchange of information. The definition of ontology and the use of semantic descriptions for data will make them inter-operable for users and stakeholders sharing and using the same ontology [11].

Autism spectrum disorders (ASDs) refer to concepts of instability that disrupt social communication, interaction and normal behavior in general. In some ways, every autistic child is unique. He or she faces serious problems with emotional balance, community interactions and communication skills; a high degree of personalizing is needed to communicate with the outside world. So far, medical science has not been able to determine the exact reason for autism; but most therapists have shown that it is the unpredictable behavior of neurons in the human brain. The prospect of the availability of IoT support for the use of services to improve the lives of children with autism and their families in society is looming; it will help teach and train autistic children basic skills and concepts in their everyday requirements.

Scalability. Because IoT generates an enormous amount of data, dealing with the volume, variety, velocity, and veracity of the data is a challenge for real-time operation and efficient data management using highly intensive, accurate analytic (Figure 4).

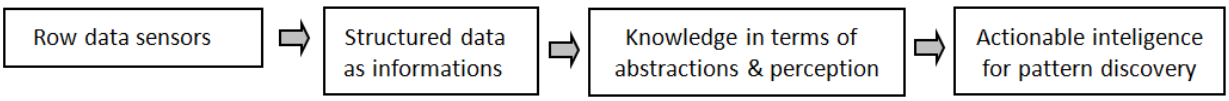

Figure 4. Knowledge hierarchy in the IoT context.

Most IoT cases use require real-time data transmission. For some of them, data transmission is even critical (health sensors, for example, or vehicle applications). Then, network operations for IoT must be secured so that data can be transmitted in real-time from the device to the destination (which could be a server, gateway or other device). The network infrastructure should ensure low delay (which could be an issue for some congested networks, such as 3G networks). Important networking challenges: network design and architecture, and dealing with appropriate protocols.

Similarly, reliability of data transfer is also of great importance for some Internet use cases. It is imperative to have a reliable network, both in terms of data transfer and in terms of security (Figure 5). Indeed, data must not be able to be intercepted and altered by malicious equipment or users. Security is also an essential requirement, along with network support, to provide a reliable IoT system [9].

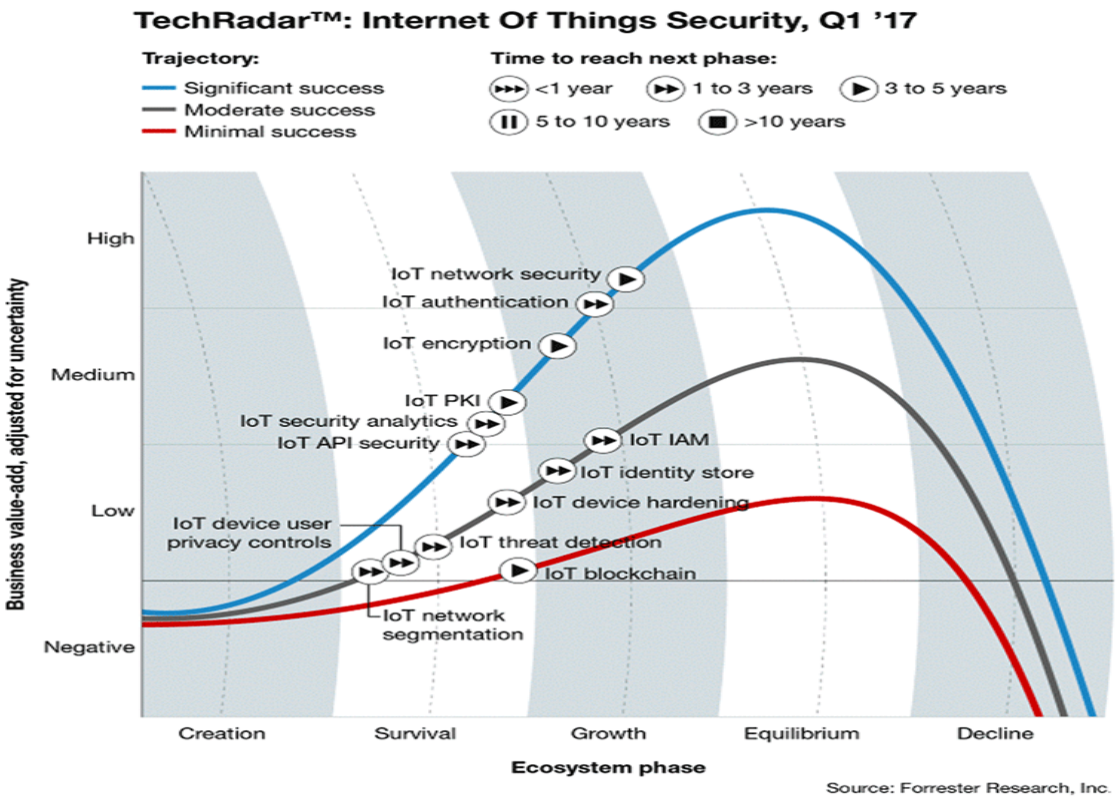

Figure 5. For 13 important security technologies of IoT, *Forrester Research* presents their prospects for future (Copyright © 2017, Forrester Research Inc.)
Quality of service.

The IoT therefore enables the connection of consumer electronic devices or household appliances, such as medical devices, refrigerators, cameras and sensors, which are part of the Internet environment. This opens the door to new innovations (that will create a type of interaction between objects and people and enable smart cities, infrastructures and services to improve quality of life and use of resources).

Coexistence issues

As IoT devices use different protocols on crowded bands, a major problem that arises is communication failure attributed to coexistence. Coexistence can be defined as the ability of wireless equipment to function when there are other devices using different protocols. Coexistence concerns are driven by three key factors: *(1)* Increased use of wireless technology for critical equipment connectivity. *(2)* Heavy use of unlimited or shared spectrum. *(3)* There are higher deployment rates of sensitive equipment such as intravenous infusion pumps, pacemakers and defibrillators. They directly influence the reliability of medical device communications.

Three techniques are commonly used to improve device and network coexistence. One technique is physical separation. Placing two networks in different locations, by each network encounters a weaker signal from the other. However, physical separation is not always practical, as is the case in healthcare environments using the 2.4 GHz industrial-medical-scientific (ISM) band. In this scenario, a large amount of IoT wireless devices across the facility can operate in this band. The second technique involves frequency separation. Essentially, interference between two networks is reduced when one network operates on a different frequency than the other - whether they are located close to each other or not.

However, frequency separation is not always effective in the 2.4 GHz band, as all *Bluetooth, Zigbee* and *IEEE 802.11 bands* use this band.

The third technique is time separation: information is sent and received at different times to avoid collisions.

What progress can be expected? (Trends)

- Voice User Interface (VUI) will be a reality;
- Real expansion of small IoT;
- Growth in data and devices with more human-device action;
- More movement to the Edge;
- More social, legal and ethical issues;
- More investments in IoT;
- IoT focus on security using Blockchain;
- The rise of industrial IoT and digital twin technology;
- Artificial Intelligence – big player in IoT;
- Standardization – still a problem.

Conclusion

The concept of combining computers, sensors and networks to monitor control devices has been around for decades, but the recent confluence of key technologies and market trends has been the catalyst for the IoT idea.

IoT promises to form the foundation of new products, processes and business models, with the potential to seriously affect both B2C (*Business to Consumer*) and B2B (*Business to Business*) markets, as well as the way we produce goods with spin-off products, including the Industrial Internet of Things and Industry 4.0.

While the ramifications are - most likely - significant, a number of potential challenges may hinder the vision, particularly in the areas of security, privacy, interoperability, standards, as well as legal, regulatory and legal issues - such as the inclusion of emerging economies. IoT encompasses not only technological considerations, but also social and political issues. IoT is fast becoming more and more a reality and there is vast scope for new designs and achievements by creators and developers.

References

1. IERC-European Research Cluster on the Internet of Things, 2013, http://www.internet-of-things-research.eu/
2. Jamil Y. Khan and Mehmet R. Yuce. Internet of Things (IoT). Systems and Applications (2019). Jenny Stanford Publishing, pp. 366.
3. Mayer S., Guinard D., Trifa V. Facilitationg the integration and interaction for real-world services for the web of things. In Urban Internet of Things: Towards Programmable Real-Time Cities (UrbanIOT 2010); Workshop at the internet of Things 2010 Conference.
4. Mayer S., Guinard D., Trifa V. SmartThings – Make your world smarter, 2013, http://smartthings.com
5. Sensinode Ltd., 2013, http://www.sensinode.com/
6. Corredor I., Bernardos A., Iglesias J., Casar J. R.: Model-driven methodology for rapid deployment of smart spaces based on resource-oriented architectures. Sensors **12**(7), 9286-935, 2012
7. Tripathy B. K., Anuradha, J. (eds.),: Internet of Things (IoT) – Technologies, Applications, Challenges and Solutions, CRC Press, Boca Raton, London, New York, 2018
8. Serpanos D., Wolf M.,: Internet-of-Things (IoT) Systems – Architectures, Algorithms, Methodologies. Springer, 2018
9. Qusay F. Hassan (ed.): Internet of Things A to Z, Technologies and Applications, IEEE Press & Wiley, 2018
10. Băjenescu Titu-Marius I. From the Internet of things (IoT) to smart cities (Sc). Journal of Engineering Sciences, 2018, no.3. https://www.doi.org/10.5281/zenodo.2557328.