Adoption, Architecture and Technology of Enterprise IoT Systems – Towards a framework of concerns in IoT environments

Mirona Popescu[1], Dan Dumitriu[1], Markus Helfert[2]

[1] Faculty of Entrepreneurship, Business
Engineering and Management, Politehnica University, Bucharest, Romania
{mirona.popescu15 ¦ dumitriud} @gmail.com
[2] School of Computing, Dublin City University, Dublin, Ireland
Markus.Helfert@dcu.ie

Abstract. Internet of Things - IoT (Internet of Things) or Internet of Everything defines a network of objects that incorporates electronic circuits that allow communication via existing infrastructure (network INTERNET), wireless or cable for many purposes, including monitoring or remote control. The existence of a web interface through which a person may access the equipment of the house is useful to increase efficiency and save resources. Both own homes as well as companies, medical services, factories, state services and communities will benefit from using connected IoT environments. These environments are characterized by information sharing between equipment, devices and humans help devices and the exchange of information between these. This research outlines the benefits brought by IoT systems adopted in companies from different viewpoints. We employ a case study in order to point to real experiences and situations. A further objective of this paper is to propose a model of architecture for the systems and examine their process of operating by analyzing the technologies used to develop such systems and the security problems that can be met.

Keywords: IoT systems, enterprises, IoT technology, machine learning, big data

1 Introduction

Invented in 1999 by British entrepreneur Kevin Aston, the concept of Internet of Things (hereinafter IoT) represents a structure of physical objects, or "things", which have electronic components, software, sensors, and Internet connections to collect and distribute data. Objects are uniquely identified, "self-aware" and can communicate with each other, locally or globally, without human intervention (based on IP connectivity). IoT also represents the omnipresent connectivity concept for businesses, governments and consumers, with their own management, monitoring, statistical computations and data analysis systems.

The above definition can be extended beyond objects, including humans and animals alike. For example, in IoT, a "thing" also refers to a person with a monitored heart implant or a dog with a microchip under the skin of his head or any other natural or artificial object to which an IP address can be attached and which is capable to transfer data over an Internet network.

Internet of Things is already omnipresent, a daily presence in many people's lives. For example, smart meters are installed in homes to coordinate and save electricity; Internet-powered cars are used from OnStar (US) or eCall (EU) system that triggers an automated response in case of an accident. Furthermore, the system allows to follow cars if they are stolen or provides technical assistance when needed; on bodies as an insertion in the smart shirt or shorts they run with, or as an auditory implant that captures the noise of the fire truck and "moans" before they can hear it.

The beginnings of internet of things were: the barcode (1974); Radio Frequency Identification (RFID) device; the incredible price drop of database storage devices required to collect, store and process thousands of bits; the emergence of IPv6, the Internet protocol that replaced the previous version, IPv4. With the new protocol, an Internet address may be available in any object that has software stored in it: the toothbrush, the coffee machine, the refrigerator, the dishwasher, etc. Technologically, IoT has become a collection of bar codes, QR codes, RFID tags, NFC (Near Field Communication) and SAAS (Machine-to-Machine) communication devices, active, Wi-Fi and IPv6.

Pan [7] investigated a unique IoT experimental testbed for energy efficiency and building intelligence, and identified the heterogeneous IoT devices as major challenges to work together as a coherent system. Similar Al-Fuqaha [8] identified that the heterogeneity of the IoT elements is challenging. To overcome the existing challenges, solution have been suggested, e.g. on communication enabling the use of wireless sensor network (WSNs) [9], enabling technologies and application services using a centralized cloud vision [10], enabling technologies with emphasis on the RFID and its potential applications [11]. However, the technologies currently used to implement IoT bring some flaws especially when it comes to security, but it is working to strengthen it to provide people and companies with the necessary safety and trust.

The aim of this paper is to outline the benefits brought by implementing IoT systems in companies regarding their field of business. Although many paper have examined the benefits and challenges of IoT, this paper specifically focuses on a corporate environment. We outline how IoT has appeared and the need of its existence in an enterprise environment that aims to evolve and improve its actual status and numbers. In our research, we employ a case study to examine IoT usage in Enterprises. Furthermore, an overview of an architecture model is proposed based on the case study findings. It illustrates the complex dependencies and workflows between its components within an IoT environment.

2 Related Work

A great amount of resources and research have been directed towards the adoption of IoT in various areas. Diverse application areas of such technologies are often summarized with terms such as ‘Smart City’, ’Smart Home’, ‘Smart Buildings’ and

lately Smart Commerce (Pan, [7]). Smart environments include smart objects, such as houses, buildings, sustainable urban infrastructure, cars, sensor technology, etc. Within these environments, through the application of semantic web technologies and intelligent applications, the systems may be personalized, responsive, and intuitive.

It is considered that the determinants of the proliferation and the success of IoT are the emergence and development of methods of artificial intelligence, machine learning and data mining. IoT is essentially a continuous flow between:

1. Body Area Network (BAN): Audible implant, smart jersey or shirt;
2. LAN (local area network): intelligent meter as the interface of our home;
3. WAN (wide area network): bicycle, car, train, bus, drone, all intelligent;
4. VWAN (very wide area network): the "smart" city, where e-services are omnipresent, without being linked to physical locations.

The increasing importance of IoT environment are due to mainly 4 factors:

(1) The exponential increase of computer capacity and the emergence of IoT could bury the world in huge volumes of unintelligible data. To solve this problem before it becomes too complex to be approached, the use of Artificial Intelligence (hereinafter AI) methods has become the favorite option of companies that try to control Big Data. The purpose of AI is to take large amounts of unstructured data - such as those produced by IoT devices - and make actionable decisions about these data. In short, AI is data-giving technology and produces significant instructions, such as commands given to IoT devices to perform specific actions.

(2) Machine learning is the global term for algorithms that, automatically or with some human support, identify patterns in the Big Data Rivers and determine which IoT device behaviors tend to create the most desirable results. Based on learning algorithms, computers can act without explicit programming. In the last decade, machine learning technology has given people, among other things, driverless cars, speech recognition, effective Internet search and a broad understanding of the human genome.

(3) Analytics and Data mining techniques as the analytical process of exploring large databases - Big Data - for finding and finding consistent patterns and / or systematic relationships between variables, followed by applying patterns detected to new data sets.

3 Concerns of IoT in Enterprises

3.1 IoT adopted by companies

The Internet of Things (IoT) is assumed to be a key part in the business world as companies progressively search for original approaches to keep up their rival edge. Research firm International Data Corp estimates that the IoT market will grow from $655.8 billion in 2014 to $1.7 trillion in 2020. Another analyst, McKinsey and Company noted there will be between 20 to 30 billion linked gadgets by 2020.

Buyers are starting to see the benefits of having their devices linked to each other and controlled remotely, associating and matching up different gadgets going from their wellness trackers to autos to home surveillance cameras. Companies all over the world are investing large amounts of their capital in adopting IoT solutions to become digitized and drag the advantages brought by the connected things and the data generated by them.

Additionally, IoT will benefit all types of business by reinventing industries on three levels:

Business process	Business model	Business moment
Digital technology will improve products and services, provide customized solutions, and deliver a better customer experience.	Industries will continue to merge	The need to compete with unprecedent business velocity and agility, companies must adapt to the changing landscape of their industries.

Fig. 1. Levels of a business

This research outlines a part of the advantages brought by IoT systems that are summarized in Fig2. and they are derived from the case studies discussed later in section 4.

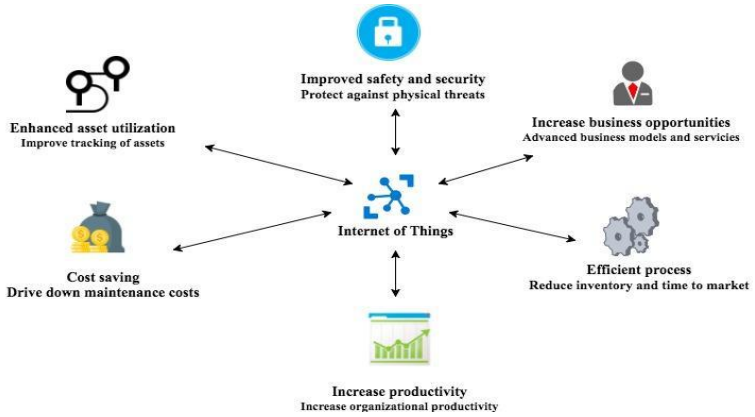

Fig. 2. Benefits of IoT (adapted after https://vmokshagroup.com/blog/6-ways-businesses-can-take-advantage-of-iot/)

3.2 IoT Architecture

The architecture of an IoT is adopting a three-tier pattern which includes edge, platform and enterprise tiers as follow:

The public networks and proximity are found in the edge tier. There is gathered all the data received from devices and transmitted to devices through the gateway or

straight from the device into the Cloud provider, using the edge services and IoT transformation and connectivity.

Cloud provider represents the platform tier, which is in charge to process and analyze the information received from the edge tier and it provides API management and visualization. It has the capacity to launch commands of control from the enterprise network to the public one.

Enterprise network defines the enterprise tier and it has the data from the enterprise, a enterprise user directory and the applications. The data goes flow to and from the network using the transformation and connectivity component. The data stored in the enterprise is gathered from structured and unstructured sources of data and real-time data that comes from stream computing.

Systems that are based on IoT are relying on application logic and control logic in a hierarchy of locations that need timescales and datasets to inform the decisions. They are parts of the code that may be executed directly on devices at the edge of the networks or in the IoT gateways that are in the proximity of the devices. Other parts of the code are carried out in the enterprise network or the provider cloud services.

Security systems and IoT governance have the role to span the architecture's elements to provide policies and control for the data and applications which are defined and enabled in the whole system.

The figure below will illustrate the process described above and the connections between all the components of an IoT system:

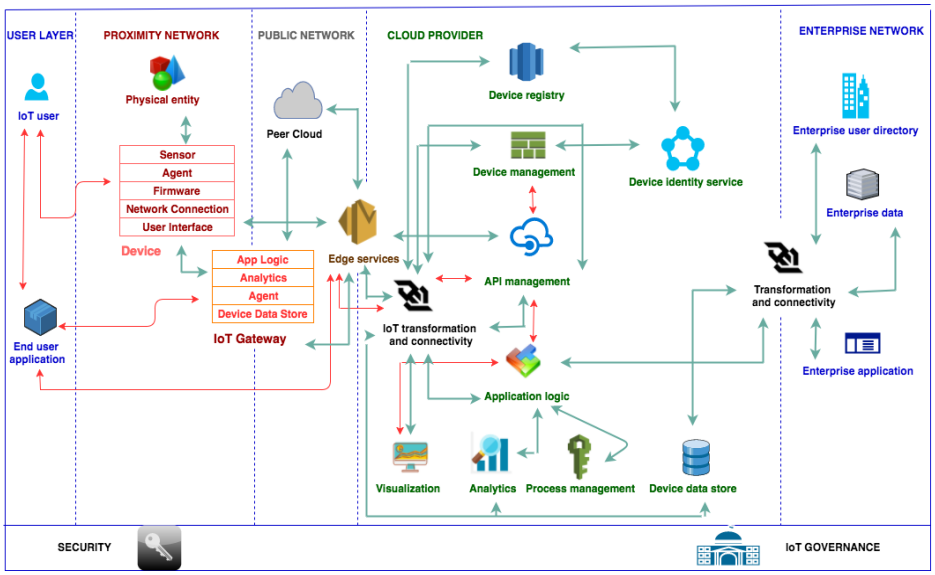

Fig. 3. IoT Overview (adapted after IBM Model of Architecture, source: https://www.ibm.com/developerworks/cloud/library/cl-grush-smart-toothbrush-bluemix-trs/index.html)

3.3 Technologies used for developing IoT systems

The basic principle behind the Radio frequency identification (hereinafter “RFID”) chips is radio wave technology. When waves pass through copper wire coils an electrical signal is generated which, in turn, powers the chip. The power obtained is used to send a reply. The following sequence of events details the aforementioned process

1. A RFID transceiver sends a pulse of radio waves. This pulse contains an identifying number
2. If an RFID tag is nearby, the pulse hits the tiny built-in antenna, creating electricity. This electricity makes the circuit "come alive" momentarily.
3. The chip checks the ID number transmitted from the receiver. If it matches, then the chip transmits its stored information in the form of a reply radio wave.
4. The transceiver picks up the reply signal from the RFID chip and the transaction is done.

The current problem with using RFID chips is that the current radio signal lacks in power. Thus, it cannot reply to a receiver in a location further than a few centimeters.

Be that as it may, the amount of energy it gets and the strength of the reply signal is a percentage of the power of the original pulse. So on the off chance that a person utilize a substantially more effective pulse, the chip can send a considerably more powerful reply. A sufficiently solid pulse can support the range to a few meters.

In this case "hacking" comes into play. With a sufficiently solid transceiver, a human could set it up to check all the RFID contributes everybody's card as they passed by. Obviously, the person should send the right code to each RFID chip to motivate it to transmit an answer. The answer may likewise be scrambled, and that can be hard to break. Be that as it may, nothing is "uncrackable", and the original RFID chips did not use any form of encryption. Some still do not.

The following table details the contents found inside the receiver data packet:

```
Card detected.
 ATQA: 04 00
 UID:  11 22 33 AA
 SAK: 8
Sector 0:
 EE 57 8E 84 B3 88 04 00 85 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF
Sector 1:
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF
Sector 2:
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF
Sector 3:
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Fig. 4. Receiver data packet content

ID is the unique identifier of the card. It can be used this for a basic check, but beware there are cards with unlocked sector 0 that can have this number reprogrammed. The number is also not really unique, only unique to a manufacturer's production run of 232 cards (for cards with a 4-byte UID). This might be fine depending on what you are doing with it.

ATQA indicates the type of the card and SAK indicates the manufacturer. More details can be found inside the ISO/IEC 14443 Type A document.

The sectors are the data storage to a card. The sector 0 is typically write protected as that stores the information presented above. If you look at your dump you can pick out some of these values in there.

The remaining sectors are available for storage on most cards. However, 16 bytes at the end are reserved for access control to the data. This includes two keys of 6 bytes each and 4 bytes that control what authenticating with these keys allows you to do with the data (read/write/increment, etc.). A new card has keys consisting of 6 0xff bytes.

If security is concerned, one or more sectors of the card need to be populated with additional data to match against beyond the UID. To authenticate a card, the ATQA, SAK, and UID need to be used to look up the read key and expected data in the card, and to authenticate the sectors with the data that should be matched, in the end a compare is done between what is found inside the card to what you is already stored.

As RFID has been around for a while, the technology has matured, and has spun off a newer technology: near-field communication (NFC). The emergence of NFC seems

to have also sparked confusion. What's the difference between RFID and NFC? RFID is a one-way process. Information is transmitted from an encoded memory chip (known as a "smart tag") via an antenna to an RFID reader. There are two types of RFID tags: active and passive. Active RFID tags contain a power source, so they can broadcast a signal, up to 100 meters away. This capability makes RFID a strong choice for asset tracking. Passive RFID tags have no power. They're activated by an electromagnetic signal sent from the RFID reader. The signal doesn't travel as far as active RFID, so they're used for short read ranges. Passive RFID falls into one of three frequency ranges: Low frequency: 125-134.2 kHz High frequency: 13.56 MHz Ultra-high frequency: 856-960 MHz NFC is based on RFID protocols. The devices run at passive RFID's high frequency. NFC reads smart tags because, like RFID, it features a read/write operation mode. But NFC goes farther than RFID. The technology has two-way communication—unlike RFID's one-directional limitation—using one of two modes: card emulation and peer-to-peer (P2P). For example, a smartphone enabled with NFC (and many of them are nowadays) can pass information back and forth to another NFC device. Contactless payment is an example of card emulation mode. Any time you redeem rewards points via your phone, you're also using NFC's card emulation feature. P2P comes into play when you "bump" your mobile device with another one to share information. Maybe you're passing music back and forth, swapping special deals, or playing a game with the friend sitting next to you. You can even tap your device with a router, to get on that network without having to use a password. NFC will soon likely replace QR codes in some advertisements and promotional materials. Consumers will no longer have to scan a QR code to get to the intended location, but can simply use the NFC mode to instantly get the information that the advertiser wants them to have. There is still plenty of space across today's industries—from retail to manufacturing, transportation to healthcare—for RFID's one-way communication, but NFC is paving another path along the ever-winding information highway.
[http://www.aaarfid.com/UploadFiles/RFID%20VS%20NFC.pdf]

4 Case Studies

Beyond connecting devices to IT systems, the true value of IoT is the ability to track, almost in real time, the inherent qualities or relationships existing in data that are always growing in volume, speed and variety. This section highlights some sectors or industries whose activities were influenced by IoT systems.

Asset tracking had been widely welcomed by the O&G industry. "There is dependably an inclination that insufficient resources are being conveyed rapidly enough," says Henry Rosen, senior vice president of sales and marketing for Geoforce, Inc., an O&G equipment asset tracking and utilization solutions provider. "With the move from RFID implementations to Global Positioning System (hereinafter GPS) technology and IoT arrangements, investment funds have hit endeavor adopters' primary concerns in two ways: working and capital uses. For instance, working expenses are lessened with fuel investment funds and diminishment in man hours; and

capital expenses are decreased with expanded volumes of turns and speed of utilization."

Consider the instance of an O&G rental hardware supplier battling with the expenses of dealing with its remotely conveyed resources. Given the multifaceted nature of the gear, experts needed to research client complaints on location, regularly spending time in between sites. Sensors were put on basic parts of the hardware that would automatically send alarms if gear related issues occur and give enough information to specialists to permit some remote investigating and determination. Site visits diminished by 50 percent, reducing personnel, vehicle, and fuel costs. Furthermore, the measure of time required for issue solving dropped from hours to minutes, bringing about less machine downtime. With bring down workloads, specialists could be conveyed to different parts of the business.

IoT can possibly empower O&G organizations to investigate and find new resource locations in much deeper and complex deposits. Sensor gadgets used on-field at exploration sites can assemble and transmit seismic information to a focal observing area, making information streams that may give new understanding into potential new sources. IoT arrangements may give more noteworthy accuracy to reveal potential O&G deposits at bigger depth underneath the earth's surface, possibly enhancing the likelihood of new disclosures and taking into account better resource/hardware and workforce arranging.

Another possibility is to look at how as an oil field administrations organization may focus on its client connections by utilizing the ongoing information spilling out of oil generation clients, joined with inner gear execution information and freely accessible products information. The oil field administrations organization could utilize the data to screen clients production rates relative to fluctuating energy prices to anticipate equipment needs by geography and potentially offer new, valuable services.

Telematics and car pool maintenance

For companies that keep up car pools, telematics can make strides vehicle operations to lessen hazard and costs and also enhance client satisfaction. Constant upkeep and hazard administration can offer assistance organizations guarantee that items and administrations are in great working request. GPS recipients can speak with electronic GSM gadgets introduced in every vehicle to permit endeavors "to screen the area, developments, status, and conduct of a vehicle or pool of vehicles," as indicated by Stein Soelberg, executive of advertising at KORE Telematics. Such arrangements can identify issues in vehicles before they are utilized. For instance, one maker of cranes and heavy machinery put sensors in tires to decrease the danger of machine failure. The sensors permitted consistent checking of tire weight with the goal that the maker could foresee potential imperfections and proactively settle them.

Telematics arrangements can possibly help vehicle makers get a constant stream of rich insight about their vehicles. As IoT networks collect copious amount of information produced from the pool, it can empower organizations to disentangle and present new ideas or highlights in their current product line-up. For instance, the sensors in heavy machinery hardware can give rich data back to the maker about how and where

the item is utilized and how that influences execution over its lifecycle. This knowledge may prompt item configuration changes. It additionally yields knowledge into clients' organizations, which the producer may offer back to the client as a form of potential feedback regarding the current contract.

mHealth and remote wellbeing observing

Pete Celano, director of consumer health initiatives in the Innovation Group at MedStar Health, has seen firsthand the advantages of IoT arrangements in medical services and how mHealth and remote wellbeing arrangements will upset medical services through guidance ahead of time and preventive care. "In a machine-to-machine interoperability case, the potential outcomes of remote medical gadgets are changing remote patient observing, particularly as there are structural movements occurring in the medical services industry." Hospital frameworks, for instance, take advantage from additional clever medical hardware that upgrade preventive care through new sorts of medical sensors that empower remote, constant observing of imperative wellbeing related measurements, independent of where the patient is found.

Celano depicts how a patient at home "can transmit wellbeing related information to the cloud by means of a non-stop remote system service, giving early-cautioning signs to facility's nurses that the patient is in linked to, or going into pressure." Medical experts can react with fitting actions. "During a time where doctor's facilities are getting to be payers as well, there is a need to oversee healing center confirmations proactively. Progressively, if suppliers do not provide results, there is no replace for the old test-heavy, experience based model and implies the smart medical services frameworks are hustling to make programs that shield patients from winding up in the crisis room."

This shrewd observing capacity prompts other human services administrations and medications, for example, cutting edge wellbeing dashboards and health centers. Market revenue for IoT developments in social insurance was evaluated at $10.6 billion out of 2012 and is relied upon to twofold by 2016.

Remote wellbeing checking starts to upset the conventional treatment condition and the occurrence based model. The blend of wearables and other intelligent hardware that enables a person to catch, track, break down and share information about themselves, will open up considerably more problematic issues: the individual, as opposed to the social insurance supplier, will claim the information about his/her body. Wellbeing and health suppliers will utilize the information to offer more customized treatment plans in light of the person's specific circumstance and reactions to past measures. People will associate with a differing biological community of health suppliers who can enable people to obtain insight out of their information to enhance wellbeing and better utilize specialized medical services suppliers when they are not well.

IoT can possibly empower oil and gas, transportation and healthcare organizations to expand and find new resource locations, to disentangle and present new ideas or highlights in their current product through telematics arrangements for companies that keep up car fleets, as well as having a significant impact in the development of preventive care.

5 Concluding Remarks and Future Research

The Internet of Things is a paradigm shift and an ontological change. The fundamental notions of what it means to be human and what it means to be "in humanity" are based on subject-object dichotomies. IoT introduces a third dimension in the current existential relationships: Big Data, specific algorithms, and a realistic scenario always present in any object-subject interaction. If we are to refer to the "next epochal invention" of mankind, IoT is just as important as the fire or the book - a paradigm shift, a disruptive event, the creation of a new vision of the present times.

There is a myriad of areas where IoT technologies are currently applied or will soon be applied: intelligent homes, smart cities, automotive, health, etc.

The biggest advantage of using IoT technology is savings in city budgets. Mixing IoT systems with Big Data could save US 1,200 billion dollars. Installing intelligent transport systems in major cities (e.g. New York, Chicago, Los Angeles, San Francisco) would contribute with 800 billion a year starting in 2030. Other areas where smart cities will get spending cuts are water and energy consumption, domestic and industrial waste management, public safety (firefighters, police officers, rescuers, and traffic controllers) or intelligent buildings (e.g. Seattle is a world leader in its efforts to build buildings with low energy consumption).

In the public smart cities sector, it can be also met IoT devices that fulfill a multitude of roles - from monitoring the level of rivers to triggering flood alerts, identifying different types of offenders, etc.

Intelligent cities technologies will cost US for example 27.5 billion by 2023, and the number of these cities will increase to 88 in 2025, according to a report made by the New Jersey Institute of Technology (NJIT). Intelligent city data will be processed and analyzed to determine how to improve the quality of life in each city, from managing financial resources to fighting crime, and so on.

Implementation of IoT on a global scale, affecting billions of people and devices, has not only benefits. Two aspects - cyber security and protection of personal privacy - seem to be the essential risks that IOT is currently facing. Secondarily, there can be listed issues related to the integration, reliability and scalability of the data used.

Often, Internet connections are vulnerable regardless of their type (Wi-Fi, Bluetooth, cellular, satellite, or microwave) or how they are connected to the PAAS (Platform-As-A-Service) or other servers and services set to search, process, or receive data from an IoT application. Vulnerability classes discovered, for example, in the hydrocarbon industry include undocumented protocols, unsafe protocols, weak passwords and "backdoors" (various ways to circumvent legitimate users authentication).

The purpose of this paper is to present the relevance of IoT systems by evaluating companies that have adopted it in various domains to automate some of the processes and increase sales, leading to firm stabilization and recognition of the company through the profit obtained and the fulfillment of the consumers' requirements. Adopting them is a win-win situation for both the company and the consumer. The paper also presents an architecture model proposed for IoT systems, but also the technologies that are currently used with their advantages and disadvantages. In conclusion, the research succeeds in highlighting the importance of technology-based evolution, artificial intelligence and IoT, which is currently expanding due to the many functions that help people once they benefit from it.

Acknowledgement: This work was supported, in part, by Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre.

References

1. http://www.contributors.ro/media-tech/the-internet-of-things-iot-lumea-obiectelor-inteligente-beneficii-%C8%99i-riscuri/
2. https://www.reddit.com/r/Futurology/comments/4bgy6f/an_excellent_overview_of_the_internet_of_things/
3. http://www.businessnewsdaily.com/5450-internet-of-things-business-opportunities.html
4. http://wso2.com/library/articles/2017/02/six-business-benefits-of-the-internet-of-things/
5. https://vmokshagroup.com/blog/6-ways-businesses-can-take-advantage-of-iot/
6. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/internet-of-things-iot-enterprise-value-report.html
7. Pan G, Qi G, Zhang W, et al. (2013). Trace analysis and mining for smart cities: issues, methods, and applications. *Communications Magazine*, IEEE, 51(6), 120-126
8. https://www.ibm.com/developerworks/cloud/library/cl-grush-smart-toothbrush-bluemix-trs/index.html
9. Atzori L, Iera A and Morabito G, (2010), The internet of things: A survey, *Computer networks*, 54(15), 2787-2805
10. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M and Ayyash M (2015), Internet of things: A survey on enabling technologies, protocols, and applications, *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.
11. Gubbi J, Buyya R, Marusic S and Palaniswami M, (2013), Internet of Things (IoT): A vision, architectural elements, and future directions, *Future generation computer systems*, 29(7), 1645-1660
12. Yang D L, Liu F and Liang Y D, (2010), A survey of the internet of things, In Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010), Atlantis Press.