Szentesi, Silviu-Gabriel; Cuc, Lavinia Denisia; Lile, Ramona; Cuc, Paul Nichita

Article

Internet of Things (IoT), challenges and perspectives in Romania: A qualitative research

Amfiteatru Economic Journal

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Szentesi, Silviu-Gabriel; Cuc, Lavinia Denisia; Lile, Ramona; Cuc, Paul Nichita (2021) : Internet of Things (IoT), challenges and perspectives in Romania: A qualitative research, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 23, Iss. 57, pp. 448-464, https://doi.org/10.24818/EA/2021/57/448

This Version is available at:
https://hdl.handle.net/10419/281581

INTERNET OF THINGS (IoT), CHALLENGES AND PERSPECTIVES IN ROMANIA: A QUALITATIVE RESEARCH

Silviu-Gabriel Szentesi[1*], Lavinia Denisia Cuc[2], Ramona Lile[3] and Paul Nichita Cuc[4]

[1)2)3)] Universitatea Aurel Vlaicu, Arad, România

[4)] University College London, United Kingdom

Please cite this article as:
Szentesi, S.G., Cuc, L.D., Lile, R. and Cuc, P.N., 2021. Internet of Things (IoT), Challenges and Perspectives in Romania: A Qualitative Research. *Amfiteatru Economic*, 23(57), pp.448-464.

DOI: 10.24818/EA/2021/57/448

Article History
Received: 30 December 2020
Revised: 9 February 2021
Accepted: 27 March 2021

Abstract

One may notice that there is a lack at a national level of studies providing scientific answers to problems such as: data safety, security and confidentiality of the data, economic viability, and impact, regarding internet interconnection of devices and equipment called the Internet of objects, and in English the Internet of Things. The implementation in industry, transportation and related services of the Internet of Things system is relatively new, being known and developed by Romanian companies more in the last five years, according to our study. The scientific research carried out was based on the semi-structured interview method, recorded audio and video through the Zoom interface. Data processing of was carried out by statistical methods advanced in the R program. The data obtained within the study provides relevant information at the level of users in the analysed fields based on a qualitative research and allows the creation of a first impression on the state of the implementation of the Internet of Objects in Romania, which represents the basis for the initiation of more focused quantitative research on all the implications of the development and use of the interconnection of devices via the Internet or other interconnection access systems.

Keywords: internet of things (IoT), industrial internet (IIoT), semi-structured interview, perceived risks, hypotheses, IoT perspectives.

JEL Classification: O14

[*] Corresponding author, **Silviu-Gabriel Szentesi** – e-mail: silviuszentesi@yahoo.com

Authors' ORCID:
Silviu-Gabriel Szentesi: orcid.org/0000-0001-7254-040X
Lavinia Denisia Cuc: orcid.org/0000-0002-6416-259X
Ramona Lile: orcid.org/0000-0002-0021-0046
Paul Nichita Cuc: orcid.org/0000-0001-7434-3645

Introduction

The term *Internet of things* was invented by Kevin Ashton when he wanted to draw the attention of Procter & Gamble management to the usefulness of the radio frequency identification system in its 1999 presentation. Also, in the same year Professor Neil Gershenfeld in his book, When Things Start to Think, which appeared in 1999, did not exactly use the exact term, but provided a clear view of the issues IoT refers to (Gershenfeld, 1999).

The Internet of Things (English abbreviated IoT) is a network in which "objects" or devices embedded with sensors are interconnected over a private or public network. IoT devices can be remotely controlled to achieve the desired functionality (Khan and Salah, 2018). The Internet of Things (IoT) is a new technological paradigm, designed as a global network of machines and devices capable of interacting with each other (Lee and Lee, 2015). The exchange of information between devices then takes place through the network using standard communication protocols. Connected smart devices or "objects" range from simple portable accessories to large machines, each containing sensor chips(Khan and Salah, 2018). The IoT network can generate large amounts of data in different formats and use different protocols that can be stored and processed in the cloud (Chang, 2020). In the last year the use of IoT system has been accelerated and, in some cases, new systems and applications were performed. For this reason, a qualitative study on the factors that may have an influence on IoT integration in the activity of industrial enterprises in Romania and the prospects for IoT development for the next period is necessary and useful to fill the knowledge gap in this field.

Since the implementation in industry, road transportation especially for industrial purposes and related support services of the IoT system is relatively new being known and developed by Romanian companies more in the last five years (according to our study) it is necessary to obtain new data on these aspects. In order to obtain complex user-level data from the analysed fields, this study was carried out on the basis of qualitative research which allows catching a first impression on these issues that underpins the initiation of more focused quantitative research on all the implications of the development and use of IoT.

In order to develop IoT, the 5G system is important. The 5G technology represents the basis for the augmented reality and virtual reality, as well as cloud-based activity platforms that can be implemented anywhere, anytime. We can say that IoT is the anteroom of the devoting of systems of production and management of processes based on artificial intelligence. The new systems open the possibility of communicating medical risks in real time, and the results of previous studies are already increasingly being applied in Romania and other countries (Szentesi et al., 2018). The effectiveness of these research steps has now been particularly proven during the pandemic period when risks are communicated permanently, and consumers have more and more smart devices allowing a monitoring of health risks and health condition (Szentesi et al., 2018). By 2020, connected devices in all technologies will reach at least 20 billion (Mahmood, 2019).

As a dynamic socio-technical system, IoT contains well-known cybersecurity risks and endemic uncertainties that arise as IoT adoption increases and the system evolves. As recent regulatory responses begin to address IoT security risks, crucial weaknesses need to be addressed – in particular related to the feedback needed to keep up with emerging risks and uncertainties (Brass et al., 2020). This article presents issues such as: development of IoT

area in the future and new challenges for the research, for literature's revision, research methodology, results and their interpretation and conclusions.

1. The development of the IoT field in the coming period and the new challenges for research

IoT development gained a huge momentum in 2013-2020, thus there was an increase in the number of IoT devices from half to twice as many compared to traditionally connected devices(Blanter and Holman, 2020). By 2020, IoT technology will have an impact of almost 6% of the global economy and will take years for the potential of IoT to be realized (Blanter and Holman, 2020). The challenges for the implementation of IoT and the evaluation of IoT's perspectives span several areas, so we have: the lack of integrated head-to-tail solutions that offer value; lack of standards for critical aspects of IoT solutions (such as security-related ones); organizational and governmental policies that do not keep pace with technological advances; complex interoperability; companies' concern about the design and complexity of implementation (Blanter and Holman, 2020). All these aspects lead to the need to carry out studies for IoT in Romania and to the knowledge and analysis of aspects that stimulate or hinder the development of IoT in the field of industry and support services for industry.

In this period there is a development of the Internet of things worldwide and as a result there are large-scale initiatives or they are ongoing in China, Japan, the US, India, South Korea and European countries where industry, associated organisations and government collaborate on complex programmes addressing the large-scale IoT implementation (Ghaffari et al., 2019; Blanter and Holman, 2020), and from this point of view research on various aspects of IoT at this circumstance is desirable at this time.

There is a lack of national studies providing scientific answers to issues such as: data safety, security and confidentiality, economic viability, impact on Internet interconnection of devices and equipment (Internet of Things) under various aspects. The collection of quality data by the semi-structured interview method is not currently carried out at the level of Romania, and an analysis of the Internet of Things (IoT) is not sufficiently studied in terms of use, development, and implementation in Romania, and even in the European Union, compared to the USA and China and other Asian countries. The development of the Gaia-X system, an EU project proposed by Germany and France (Bundesministerium für Wirtschaft und Energie, 2020), a project to be completed in 2021 and which is taking an important step towards an European sovereign digital infrastructure will boost the development of IoT and related applications. On the other hand, there are a number of serious user concerns about the dangers of the Internet of things growth, in particular in the areas of privacy and security (Brass et al., 2020).

In the current pandemic and economic conjuncture conditions, the study on the Internet of objects from industrial area, also called industrial Internet (IIoT) is clearly required because it has great potential for almost all aspects of industrial operations, including quality control, predictive maintenance, real-time monitoring of asset status, sustainability, and business continuity. IIoT also promises increased safety, better reliability, smart metering, as well as efficient inventory management, equipment tracking and installation management. According to IBM, the latent business value that can be unlocked by the industrial IoT vision could reach up to $3.7 trillion in 2025. However, there are also numerous challenges in the adoption of IIoT, including operational complexity, connectivity challenges, service

availability, data security, diversity of connected objects, lack of ubiquitous interoperability, high cost of necessary infrastructure, complexity of large data analysis, as well as the insufficiency of Internet bandwidth and the insecurity of the current Internet (Mahmood et al., 2019), issues that of course need to be studied in detail.

Ozdemir Vural in his 2018 article, *The Dark Side of the Moon*, drew attention to the dangers of achieving full connectivity enhanced by artificial intelligence and Industry 4.0. The 4.0 Industry concept uses the Internet of Things (IoT) to connect, communicate and collect large data from sensors embedded in living and inanimate objects. When we add real-time data analysis and artificial intelligence (AI) to IoT, a state of extreme global connectivity or the so-called "quantified planet" is created. With its emphasis on system connectivity, Industry 4.0 is of interest in the manufacture of health products and the automation of services in medicine, biology, ecology, and society. But there are also uncontrolled assumptions, extreme connectivity creates an "all eggs in one basket" problem and thus the potential for complete network collapse into a domino effect when a component of a highly integrated system fails. (Ozdemir,2018).

In this context the paper contributes to the development of knowledge in the field of IoT because it makes a contextual analysis of the development and the future of IoT in Romania, it obtains qualitative information giving a first impression and picture on the IIoT situation. This data collected from Romanian companies, by semi-structured interview, allows to identify the level of integration of IoT in the activity of companies, a first capture of potential risks perceived by users in industry, car transportation and support services, or of the barriers in the implementation and use of IoT. It has been captured also the availability of the internet of objects' users (IoT) to develop in the near future this way of realization of this way of realization, management, monitoring of activities. The semi-structured interview and the coding of the results allow qualitative and quantitative interpretation of the results and a data processing on a statistical basis (Hillman and Radel 2018), through the R program. Within this sense, in this article, literature's revision has been done, and research methodology has been presented, as well as the results and the conclusions of the article.

2. Review of scientific literature

The rapid development and deployment of intelligent and IoT-based technologies (Internet of Things) have enabled remarkable technological advances for various aspects of life. The main purpose of IoT technologies is to simplify processes in different fields, to ensure better efficiency of systems (specific technologies or processes) and, ultimately, to improve the quality of life (Nizetic et al., 2020). From this perspective, the transdisciplinary and interdisciplinary approach seems increasingly necessary (Feher et al., 2019), and in this respect in 2019 at the SpliTech2019 Conference held in Croatia, a better link was made between IoT experts from different engineering professions, industrial experts and finally with academic researchers (Nizetic et al., 2020).

Another important aspect is the quality of IoT services and the concern for their standardisation for a better interoperability. The Internet of things (IoT) comprises several standards of communication network technology and most of them work in isolation from each other, for example on a system, process, department, etc. (Bello and Zeadally, 2019). However, in order to achieve the main objective of the IoT paradigm, which is to provide efficient and high-quality intelligent services, it is necessary to interoperate between different

IoT standards. Therefore, interoperability and quality assurance of services are two of the basic requirements for current and future standards operating in the IoT ecosystem (Bello and Zeadally, 2019).

The adoption and implementation of "Internet of things" (IoT) technologies leads to architectural changes to automation and industrial control systems, including greater connectivity to industrial systems (Boyes et al., 2018). In this case, the risks associated with a gradual or sudden opening of the internal system also increase the risk of external exposure (Boyes et al., 2018).

In the specialized literature diverse concerns are expressed regarding the dangers in the growth connected to the IoT implementation and development, particularly in the areas of privacy and security (Colakovic et al., 2018). Security and privacy issues are identified as key challenges in implementing IoT solutions, as there are numerous examples of threats, vulnerabilities, and risks (Qi, J., et al. 2014). Several security models and threat taxonomy models for IoT systems have been proposed (Chen et al., 2018). According to the Hewlett Packard Enterprise Research study, most problems related to the privacy of devices raised due to: insufficient authentication and authorization, lack of transport encryption, unsafe web interface, unsafe software and firmware, etc. Colakovic and Hadžialic examine the most common IoT security and privacy issues. These may include: attack detection, scalable approach, encryption, data leakage, data integrity, antivirus protection, trust management, recovery and self-recovery, access control, authentication, context awareness, standardized mechanisms and real-time protection. Security features must be incorporated at each level of the IoT architecture and effective trust management must be implemented (Adat and Gupta, 2018).

This is the reason that IoT security architecture is still under development (Sicaria et al., 2016), as well as various mechanisms developed to improve security and privacy. Security mechanisms should provide authentication, controlled access (access control), data integrity and privacy, encryption and other functions, while allowing automatic data processing based on user-configured policies and rules. These mechanisms must work in real time and must be cost-effective and scalable in order to minimise complexity and maximise usability. It should be noted that there are many key features of IoT that make it difficult to develop robust security architectures for IoT applications (Chen, et al., 2018) and for this reason these aspects must also be studied from the user's perspective. Challenges in applying IoT security risk mitigation due to physical connection, heterogeneity, resource constraints, confidentiality, high level of activities, trust management and a certain lack of preparation to ensure the security of IoT system activities are current challenges (Mohamad Noor and Hassan, 2019).

The future of IoT is based on technological developments that allow easy use of the Internet of things and a large-scale development of this device connection technology. Such an example is the traditional wireless communications technologies, such as Bluetooth and Wi-Fi, which were widely used over the past two decades (Muratkar et al., 2020). They offer various advantages, such as: higher levels of data connection, good coverage, mobility, expandability, ease of use, etc. Even in this way, traditional wireless communications solutions are expensive and also consume the battery life of devices connected to them. The Internet of things (IoT) requires devices consuming very little energy and are less bulky (Muratkar et al., 2020). Such a solution to this is the new passive technology called the Ambient Backscatter Communication System. It is a first version of a cutting-edge technology allowing wireless communication between devices by using ambient radio

frequency (RF) signals of TV and cellular transmissions. This new technology allows a very low energy consumption during communication and brings us closer to the world of IoT and its applications (Muratkar et al., 2020).

To ensure high performance and real-time reliability, new research challenges arise from both the IoT platform and the application. From a platform point of view, built-in detection devices have limited storage capacity and cannot retain many copies of data for retransmission, and in addition, both devices and IoT gateways do not have sufficient network bandwidth, neither for data retransmission nor for data replication (Wang et al., 2020). The gateway represents an access point on the network (a server or even a special network) that serves as an entry into another network.

IoT can stimulate and change the way people operate in the construction industry. There is research to find out the impact factors that influence the willingness of practitioners to adopt IoT in the construction industry in various Asian countries such as Taiwan. Studies target future issues such as: anticipated benefits that significantly influence users' readiness to adopt IoT, efforts that significantly influence users' willingness to adopt IoT, and company expectations that significantly influence users' willingness to adopt IoT (Chen et al., 2020).

4.0 industry allows for a rapid fusion of technologies that successively dissolve the dividing line between the physical and virtual worlds and is closely linked to IoT. In the age of industrial digitization, companies are increasingly investing in tools and solutions that enable technological processes, machines, employees and even products themselves to be integrated into a single network for data collection, data analysis, evaluation, company development and performance improvement. This requires simultaneous development of IoT and Industry 4.0. In Eastern European countries, such as Hungary, companies operating within 4.0 industry, linked to Internet of Things (IoT) tools, lead to more efficient production processes and high productivity and economies of scale that could lead to increased economic sustainability. In these circumstances, one may notice that, in Hungary, companies have started on the path of digitisation and investments in digitalisation, 4.0 industry and the Internet of things have already started. (Nagy et al., 2018).

Internet of Things (IoT) devices and technology are increasingly integrated into smart grids. These devices have many security vulnerabilities. To combat this, IoT protocols have been expanded with security mechanisms. However, these mechanisms shall introduce into the system additional processing which may lead to delays. These delays may affect the reliable operation of a smart power system on which prompt communication depends. Recent studies are investigating in real time the properties of the security protocols of the communications systems used (Kondoro, et al., 2021). In the industrial sector, IoT promises to reshape the entire landscape, as the value of the Internet of things business in the industrial sector has been recognized as very high one. For this reason, the Internet of things in the industrial sector, also called the Industrial Internet, often called Industrial IoT (IIoT), is becoming increasingly ubiquitous, especially as digitalisation and automation are becoming a business reality for many organisations in sectors such as production, logistics, oil and gas, water and electricity, renewable energy, mining, transportation, aviation and many others. Thus, the market opportunities for the IIOT paradigm are huge. According to research, the IIOT market is estimated to reach $125 billion by 2021. The basic philosophy behind IIoT is that smart machines are more efficient than humans in capturing, transmitting and accurately processing real-time data for market observation of business and corporate information relevant to decision-making (Mahmood, 2019). In practice, many areas of IoT applications, such as

industrial car transportation in the fleet system of trains, are related to the tracking, monitoring and transport of targets, can make extensive use of Wireless Sensor Networks (WSN) technology. The development of cloud computing technologies and the increasing increase in big-data traffic caused by the incorporation of the Internet of things (IoT) poses the problem of secure authentication. At this situation generated by the reality of the end of 2020, secure authentication of users for remote access plays a crucial role. In the future, cloud-based IoT applications will be developed to enable easy and secure remote access to the system (Deebak and Al-Turjman, 2021).

With rapid technological progress in the Internet of things (IoT) and Artificial Intelligence (AI), various human-machine touch interfaces (ITOM-HMI) have been widely developed as critical elements for providing information between people and machines in large applications. Recently, ITOMs based on wearable flexible sensors have been extensively investigated on the basis of intelligent skin in applications of physiological monitoring, motion detection, robotics, healthcare and virtual reality / augmented reality (Tang et al., 2021). With the rapid growth of distributed renewable energy and the development of IoT-related technologies, energy can be transferred bidirectional and traded flexibly in an open market, which opens up a new operational field for the extensive use of IoT (Wu, et al., 2021).

An important aspect which worth further studying is related to concerns about the environmental and human health impact of the Internet of things (IoT). Greater social responsibility, in English Corporate Social Responsibility (CSR), towards the natural environment and public health, due to side effects that could occur due to the use of these technologies Industry 4.0, the Internet of things and the use of the 5G network, are important research concerns in Romania (Feher et al., 2019). Thus, CSR contribution to the development of society is a subject of extensive debate in the literature (Crișan-Mitra and Stanca and Dabija, 2020). Despite the proliferation of CSR in academic and organisational spheres, empirical evidence in this area remains limited, especially in the context of emerging countries such as Romania. (Crișan-Mitra et al., 2020).

3. Research methodology

Starting from the research literature review within the research, we sought answers to issues such as: 1) some barriers that are considered relevant, by involved persons and decision-makers, in the integration of the Internet of objects into industry, in transportation for industry and support services. Support services consist of information and communication technology (ITC) activities to support and implement IoT in the work of organizations, as well as activities of specialized companies providing IoT solutions and services to industrial and domestic consumers; (2) what is the perspective of the decision-makers involved in IoT on the factors influencing the decision to extend IoT into industry, transportation and support services, the risks and the perception of the existence of barriers to implementation, such as staff scarcity; 3) the influence of the level of knowledge of IoT, on the one hand, and familiarity with the benefits of the Internet of Things, on the other, on the expansion of the Internet of Things in industry (IOT); 4) what is the view of users on the prospects for the development and implementation of IoT in their own activity in the industry, car transportation for industry and support services regarding support and implementation.

The research methodology used by the research team is based on the semi-structured interview technique and the use of a communication interface, in this case the Zoom platform.

The interviews have been archived audio and video and led to the creation of the information/data base for an in-depth study. Since the research methodology adopted presents aspects relevant to each situation analysed, we have opted for the semi-structured interview method.

During this pandemic period, we chose to record online interviews, an interview lasting between 30 and 40 minutes based on a preconfigured interview structure named in the semi-structured literature (Hillman and Radel 2018), the semi-structured interview offers the possibility of drawing association tables between qualitative variables which allow quantitative analyses such as the chi-squared independence test and the calculation of the Cramer's V coefficient (Lile, Szenteși et al., 2015). Interviews were conducted by the research team during the fourth quarter of 2020. We have launched the invitation to participate in this research for 60 companies from across Romania. We received a favorable response from 28 companies, of which 25 people, representatives of the companies, actually participated in the study, who gave the interview which was recorded audio and video. The persons interviewed are CEOs, managers of various levels in the technical and economic field or various experts from firms (Annex 1). The analyzed companies operate in the field of industrial production, car transport for industry and support services such as Internet of objects software (IoT). Information on businesses and respondents is listed in Annex No. 1.

The questions are semi-structured, with possibility of a free answer option, and they are the following:

The questions formulated and addressed in a structured way to users were:

- You own in your company/organization part/devices/machines/installations that can be operated over the internet?
- Can you give an example of such a device in your company/organization?
- How do you use this device in your company/organization?
- How familiar are you with the Internet of things (IoT) concept or devices connected over the Internet?
- How many types of devices/apart/cars/installations/that can be operated over the internet do you have in your company/organization?
- How many devices/apart/cars/installations/that can be operated over the internet do you own in your company/organization?
- What is the aspect that holds you back/concerns most about the use of these devices/apart/machines/installations?
- What are the obvious advantages of using the Internet of Things (IoT)?
- What are the issues/issues that make you most unhappy with the use of these devices/apart/machines/installations in the IoT system?
- Do you think that in the future it is also right to implement these IoT solutions at European level?
- Have you heard about GAIA-X, the EU's recently launched European net management and Google search engine project?

- Do you want to develop and implement more and more IoT solutions in your business in the near future?
- Do you consider that the advantages compared to the disadvantages/risks of implementing an IoT system are on the side of the advantages?
- In the sector where you operate this system is suitable/fits very well:
- On a scale of 1 to 100 (percentage) how safe are you in the future development or large-scale implementation of the IoT system in your company/organization?
- Do you think this IoT will transform the way we live and work over the next 3 years?
- How Pandemic Sars-Cov-2 influenced the development of the Internet of Things in your enterprise

In addition to the aspects mentioned in the specific reviewed literature, such as the risks and prospects of IoT development, we have proposed to verify also some hypotheses with regards to issues reported by respondents during the interviews which are interesting or sensitive to the IoT problem in Romania. The questions raised in the interview were aimed at capturing the qualitative aspects of IoT in Romania and the foundation of the testing of some hypotheses. Based on the responses obtained on the basis of the semi-structured interview, we have encoded the data, and a centralization and aggregation of data was carried out for qualitative analysis and further quantitative processing.

The hypotheses proposed by the research team are:

H_1: The Internet of Things is implemented in industry on a smaller scale than in transportation and support services, namely there are fewer types of devices.

H_2: The level of implementation of IoT in the organization depends on the familiarity with the concept of IoT.

H_3: The large-scale implementation of the IoT system in the company/organisation depends on the benefit (benefit)/risk(cost) ratio.

H_4: The most important risk perceived by respondents (over 50%) is related to the possibility of computer attack on devices and data when using IoT.

H_5: The number of Connected Devices IoT depends on the size of the company.

H_6: Respondents' impression of how we will live and work over the next 3 years also depends on their knowledge of the Gaia X project.

H_7: A large number over 3, respectively from 4-7 problems that displease respondents regarding the use of these devices/equipment/cars/installations in IoT system affect the desire to develop and implement more and more IoT solutions in the company's activity.

H_8: Respondents' impression that IoT will transform the way we live and work over the next 3 years also depends on work and remote work control/telework/homework within the organization.

H_9: Respondents' impression of the development of IoT and how we will live and work over the next 3 years also depends on the influence of the pandemic and Covid 19 disease.

With the data obtained, a database was created and they were processed through the R econometric analysis program. The information was encoded and standardized and advanced data processing as well as a descriptive statistic was carried out. Statistical assumptions related to production and service activity were tested on the basis of the chi-squared test and the correlation coefficient Cramer's V, for a significance threshold of 5%.

4. Results and interpretations

The data were analysed quantitatively and qualitatively, encoded for easier econometric processing and for the development of descriptive statistics.

A total of 25 valid interviews were recorded. The data set consists of 19 men and 6 women in senior positions in companies whose activities, such as automotive, logistics or electrical engineering, are implementing IoT systems. First, we divided these areas into 2 groups, production (e.g. production of electrical parts, production of medical devices, etc.) and services (e.g. software development, logistics, etc.). There are 12 people in the production category and 13 in the service category. In general, their level of understanding of the subject in question was high so 12 people said they knew the subject very well, 6 well, 6 enough and only 1 person was not having enough knowledge on the subject. Furthermore, we do notice that people in the service category better evaluate their understanding of the IoT topic than the production category. The main advantage identified both by services category and production one is acting and control from distance of those devices through IoT system.

But in terms of disadvantages, while both groups mention the resistance of the device in critical situations as a significant problem, for the production group the rarity of staff with adequate qualifications is another big disadvantage and the possibility of a system error for the service group. In addition, both subsets agree that the major risks of implementing IoT on a scale are data protection issues that can reach service providers or cyber-attacks.

Both subsets want to deploy more IoT devices in the future, but most of them consider a medium term for this event to take place. On a scale from 0 to 100 it has been checked how sure are respondents that this implementation takes place. The overall average is 78.71%, so we then check whether the average response is different between the two groups: production and support services (Figure no.1). The result of testing the nine hypotheses proposed in the methodology is found in Table 1, where the relevant statistic values are synthetically presented for their confirmation or denial.

Table no. 1. Result of testing the hypotheses

Hypotheses	Chi-squared value	Cramer's V	Chi-squared p-value (<0,05)
H1	0.02	0.04	0.89
H2	2.52	0.32	0.11
H3	4.17	0.41	0.96
H4	13.79	0.53	0.001
H5	6.29	0.36	0.17
H6	1.14	0.21	0.29
H7	0.20	0.09	0.65
H8	5.21	0.46	0.02
H9	7.14	0.54	0.03

Source: own research

The data have been processed in programme R and the results obtained allow an analysis of the assumptions made. Hypothesis H_1: The Internet of Things is implemented in industry on a smaller scale than in transportation and support services, namely the answers at the Q5 question associated with the answers at question Q17, namely the fact that there are fewer types of devices in the industry than in support services is an unconfirmed hypothesis. Based on the result obtained on the test, Cramer's V coefficient is 0,04 and indicates no association. H_2: The level of implementation of IoT in the organization depends on the familiarity with the concept of IoT. According to Cramer's V and chi-squared hypothesis H_2 is not confirmed, thus the level of implementation of IoT in the organization does not depend on the familiarity regarding the concept of IoT. The H_3 hypothesis assumes that the large-scale implementation of the IoT system in the company depends on the benefit-risk ratio. The value of the chi-squared test is greater than 3,814 (table value), but we do not reject the null hypothesis since the p value of the test is 0.96, being above the significance level of 0.05. Thus, a clear link between the desire for implementation and the benefit-risk ratio is not confirmed. Hypothesis H_4: The most important perceived risk of respondents (over 50%) is related to the possibility of computer attack on devices and data when using IoT. The association between Q7abc and secure implementation over 90% at Q15 is confirmed. It is found that the p value of the chi-squared test is 0.001 and Cramer's V correlation coefficient is 0.54 and therefore there is a strong relationship between the perceived risk and the desire to develop new IoT systems and applications.

It is noted that there is no relationship between the desire to implement more and more IoT solutions in the company's activity and the number of problems that displease respondents regarding the use of devices in ioT (H_7)system, between the respondents' opinion on the impact of IoT on the way of life and the knowledge of the Gaia X project (H_6) and between the number of IoT devices connected and the size of the company (H_5), since the p values of the chi-squared tests are 0.65, 0.29 and 0.17; assumptions H_5, H_6 and H_7 are infirmed. Hypothesis H_8: The impression of respondents on how we will live and work over the next 3 years also depends on the work and control of remote work within the organization, namely Q16 related to Q24, is confirmed. Based on the chi-squared dining test, the p value of which was 0.03, it results that there is a relationship between the fact that IoT technology will change society over the next three years (Q16) and remote work control within the company. Cramer's V correlation coefficient is 0.46, which is a fairly strong association. Hypothesis H_9: Respondents' impression of how we will live and work over the next three years also depends on the influence of the pandemic and Covid19 disease, respectively Q16 related to Q25 is also confirmed. In this case, the null hypothesis is: the two variables are independent, and the alternative hypothesis is: the two variables are dependent. We reject the null hypothesis because the p-value of the test is 0.03, being below the significance level of 0.05. We conclude that they are not independent, so we continue to check how strong this relationship is by calculating Cramer's V correlation coefficient for the two sets. We get a value of 0.54, which is a strong association.

It also checks the normality of the Q15 dataset, the certainty of the future implementation of IoT, by performing a Shapiro-Wilk test. We take the null hypothesis H_0: the population is distributed normally and the alternative hypothesis H1: the population is not distributed normally. The p-value of 0.0016 of the test suggests that we should reject the null hypothesis and conclude the same, this set was not collected from a normal distribution. We checked the two groups associated with production and services respectively. We used a non-parametric Wilcoxon test to check the median of the two associated groups. We take the null H0

hypothesis: the two data sets, namely services and production, have equal medians and the alternative H1 hypothesis: the two data sets do not have equal medians. The p value of the test is 0.031, which is less than the alpha significance level = 0.05. We can conclude that the median certainty of the services category regarding the future implementation of IoT in their company is significantly different from the median certainty of the production-related areas;

We perform a chi-squared test for specific pairs of variables, as Q5-Q12, Q6-Q12, Q18-Q25, Q15-Q4, Q14-Q16, Q14-Q15 to check if there are categorical variables with a significant correlation between them. We have as a null hypothesis H0: no relationship exists between category variables; are independent and the alternative hypothesis H1: the variables are not independent. We conclude that there is no relationship between how many IoT devices and how many types of devices an enterprise has (Q5 and Q6) and their likelihood of deploying multiple devices in the future (Q12), since their chi-squared test values are 0.16 and 0.19 respectively, so we can reject the null hypothesis at a significance level of 0.05. The size of the company is also independent of the influence of the Sars-Cov-2 pandemic, we do not reject the null hypothesis that the two variables are independent because the p value is 0.20.

A chi-squared test has been performed regarding the certainty of implementing in the future and IoT (Q15) and the suitability of IoT technology in the activity area of the company (Q14). The null hypothesis H0 is that the two variables are independent, and the alternative H1 hypothesis is that the two values are dependent. We reject the null hypothesis as we get a p-value of 0.026, which is below the significance level of 0.05. We conclude that those are not independent, thus we keep checking how strong this relationship is by calculating Cramer's V correlation coefficient for the two sets. We get a value of 0.81, representing a strong association.

Finally, for the relationship between the suitability of IoT technology in their field of activity (Q14) and the respondents' opinion that IoT technology will change society in the future (Q16) we are again calculating Cramer's V correlation coefficient. We get a value of 0.53 which is a strong association between the two category variables. Question Q9 finds that 36% of firms have problems with the lack or rarity of staff with adequate qualifications which is not mentioned in the literature as one of the barriers in the implementation of IoT by companies, although in Romania this aspect is considered by respondents quite important. Recent studies are investigating in real time the properties of the security protocols of the communications system used (Kondoro et al., 2021), which leads to certain delays and some uncertainty in the management of some production systems, which is partially confirmed by this research although in our study it is found that the main problem is the protection of devices and data against hackers and other organizations and less aspects of system management. In some firms there is a reluctance to implement IoT widely due to poor system reliability and sometimes connection problems that increase insecurity (28% of respondents) issues that have been mentioned by other authors (Mohamad and Hassan, 2019). We find that the average number of devices used in the IoT system per organization/firm is about 6.6 devices (Figure 2) a relatively small comparative with countries such as Hungary (Nagy et al., 2018).

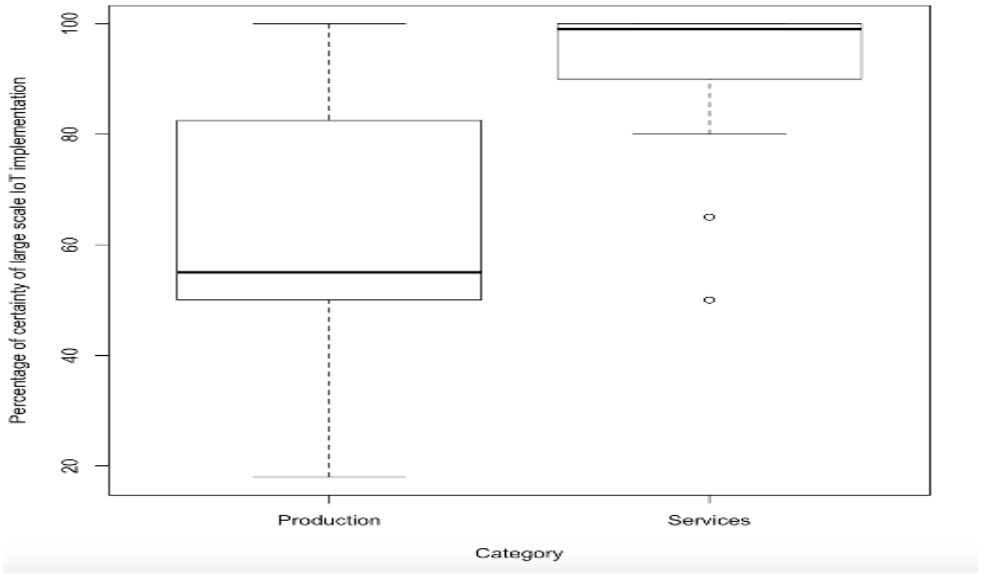

Figure no. 1. Certitude of IoT development according to activity subareas
Source: own research

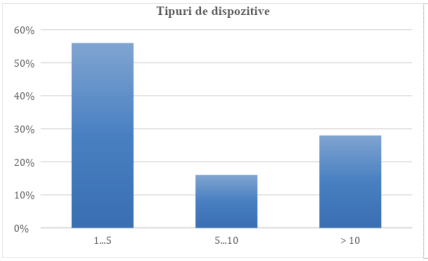

Figure no. 2. Number of devices per company
Source: own research

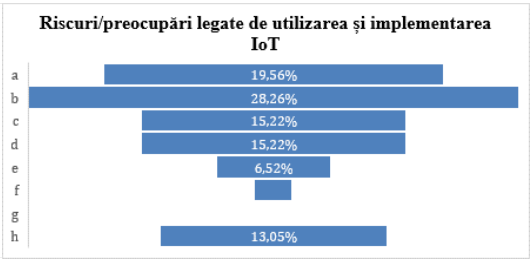

Figure no. 3. Risks percentage analysis per risk type
Source: own research

Conclusions

a. Theoretical contributions. The study is important for business and academia because it brings to the attention a first perception of the use, barriers and risks associated with use as well as the prospects for the development of the Internet of Things in the industry and support services (IIoT) in Romania. Information has been learned about the impact of remote and home office work and of the pandemic on how we will live and work over the next three years (H_8 and H_9, confirmed). The implementation of IoT in the opinion of the company representatives also depends on how much it fits at the moment the use of an IoT system in their field of activity. In Romanian companies there is, according to h_2 conclusions, a definite relationship between the level of implementation of IoT in the organization and the familiarity regarding the concept of IoT which indicates a determination at the decision-making level to implement IoT even if there is no high familiarity regarding the industrial

internet of things (IOT). Our study shows that 92% of the firms analysed are very familiar with this concept and 8% are well or sufficiently familiar. Most of these devices are not used in a modern system and fully integrated into the company's business. 88% of the connection is made by wire (internet cable) or wi-fi, but there are also companies that have more advanced systems at their disposal. In the analysed companies there is a fairly high percentage of 56% that have a maximum of 5 types of devices connected to the IoT system, 16% between 5-10 devices and 28% with more than 10 types of devices, which denotes a fairly advanced use of IoT in this last category. Regarding the risk and retention aspects of the extended use of IoT, companies put first, aspect which corresponds to the presentation of risks regarding IoT from reviewed literature, with a percentage of 28,26%, uncertainty regarding the protection of devices/devices/machines/installations that can be attacked informatically (by hackers or other organizations), the second place of preference and uncertainty, with a percentage of 19,56% the protection of the company's data that can reach internet providers or service generators. This risk to service generators is also perceived to some extent due to the lack of information on the European Union (EU) Gaia-X project which will become operational in 2021 and will provide services to European Union companies in compliance with data protection of companies in accordance with European Union law. Thirdly, it is pointed out the concerns about the possibility of third parties entering through the net connection in the management/ administration/ management of the company and high acquisition/implementation/high implementation time (15.22%). Uncertainties were also expressed as to effective profitability (6.52%) as well as concerns about the environmental and human health impact (2.17%), and 13.05% of views as diverse as dependence on suppliers or the difficulty of implementing a truly efficient system.

b. Managerial implications. An important aspect of the research is that the risk in various forms represents a significant restraint to the expansion of IoT and IIOT in Romania, which is in correlation with the concerns and barriers to the development of IoT mentioned in other works. Issues such as: protection of company data that can reach internet providers or service generators, protection of devices that can be informatically attacked (by hackers, other organisations), the possibility of third parties to enter through the net connection into the gestion/ management of the company, are concerns of the majority of the company's representatives, while concerns about issues such as: high acquisition and implementation costs, high implementation time, uncertainties about effective profitability, concerns about the environmental and human health impact, other ethical and/or legal issues still unresolved, etc. represent 44% of concerns. Thus, the assumption of the significant influence of risks and uncertainty on the implementation of IoT is confirmed. In particular, there is a significant risk of leaking information through IoT and the possibility of cyber-attacks by hackers or other organizations. Another important aspect to be mentioned is the fact that in some companies there is a hold in terms of the wide implementation of IoT due to poor system reliability and sometimes connection problems that increase uncertainty (28% of respondents). The study found that 36% of the firms analysed had problems with the lack or rarity of staff with adequate qualifications, indicating the need to accelerate staff training at company level and to initiate the establishment of the academic specialisations needed to support the development of IoT.

c. Limits. Qualitative research carried out on a relatively small number of threads gives a first impression on the state of implementation of IoT in Romania, but it is necessary to initiate more focused quantitative research on all the implications of the development and use of the interconnection of devices via the Internet or other systems of access to interconnection.

d. Perspective. In conclusion, the qualitative study, on the factors that may have an influence on the integration of IoT in the activity of industrial enterprises in Romania and the prospects

of IoT development in the next period, provides a first impression on the use of IioT in the Romanian industry and support services, the barriers to the use and implementation on a larger scale of IoT and provides a first forecast of the future on the development of IoT and how we will live and work in the coming years. From the literature review we conclude that IoT is a forward-looking technology but over average duration it can only develop with a substantial input from artificial intelligence systems.

References

Adat, V., Gupta, B.B., 2018. Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, 67(3), pp.423-441.

Bello, O., Zeadally, S., 2019. Toward efficient smartification of the Internet of Things (IoT) services. *Future Generation Computer Systems*, 92, pp.663-673.

Blanter, A., Holman, M., 2020. Internet of Things, 2020: A Glimpse into the Future. [pdf] Available at: <https://aradinfocenter.com/wp-content/uploads/2017/07/A.T.%20Kearney_Internet%20of%20Things%202020%20Presentation_Online.pdf > [Accessed 02.10.2020].

Boyes H., Hallaq, B., Cunningham, J., 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, 101, pp.1-12.

Brass, I., Sowell, J., H., 2020. Adaptive governance for the Internet of Things: Coping with emerging security. Regulation & Governance, pp.3-8.

Bundesministerium für Wirtschaft und Energie, 2020. *GAIA-X vollzieht wichtigen Schritt hin zu einer souveränen europäischen digitalen Infrastruktur*. [online] Available at: <https://www.kooperation-international.de/aktuelles/nachrichten/detail/info/gaia-x-vollzieht-wichtigen-schritt-hin-zu-einer-souveraenen-europaeischen-digitalen-infrastruktur/> [Accessed 6 October 2020].

Chang V., Munoz, V. M., Ramachan M., 2020. Emerging applications of internet of things, big data, security, and complexity: special issue on collaboration opportunity for IoTBDS and COMPLEXIS. *Computing*, 102, pp.1301-1304.

Chen, J-H., Ha, N., T., T., Tai H-W., Chang, C-A., 2020. The willingness to adopt the internet of things (IoT) conception in Taiwan's construction industry. *Journal of Civil Engineering and Management*, 26(6), pp.534-550.

Chen, K., Zhang, S., Li, Z. et al. 2018. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*, 2, pp.97-110.

Colakovic A., Hadžialic M., 2018. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, 144, pp.17-39.

Crișan-Mitra, C., Stanca, L., Dabija, D.C., 2020. Corporate social performance: an assessment model on an emerging market. *Sustainability*, 12(10), pp.7-21.

Deebak, B., D., AL-Turjman, F., 2021. Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Generation Computer Systems*, 116, pp.406-425.

Feher, A., Tabita, A., Orboi, M.D., Raicov, M., Banes, A., 2019. Education as basis of sustainable development, *Proceedings of the 9th International Scientific Congerence Rural Development 2019*, pp. 376-380.

Gershenfeld, N., 1999. *When Things Start to Think*. 1st ed. New York: Holt Paperbacks.

Ghaffari, K., Lagzian, M., Kazemi, M., Malekzadeh, G., 2019. A comprehensive framework for Internet of Things development A grounded theory study of requirements. *Journal of Enterprise Information Management,* 33(1), pp.23-50.

Hewlett Packard Enterprise Report, 2015. *Internet of Things research study*. [online]. Available at: <https://www8.hp.com/us/en/hp-news/press-release.html?id=1909050#.YEHpQugzY2w> [Accessed: 02.10.2020].

Hillman, W., Radel, K., 2018. *Qualitative methods in tourism research, Theory and Practice.* 1st ed. Bristol: Channel View Publication.

Khan, M.A., Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems,* 82, pp.395-411.

Kondoro, A., Dhaou, I.B., Tenhunen, H., Mvungi, N., 2021. Real time performance analysis of secure IoT protocols for microgrid communication Future Generation Computer System. *Future Generation Computer Systems,* 116. pp.1-12.

Lee, I., Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), pp.431-440.

Lile, R., Szentesi, S.G., Rusu, S., Csorba, L., Bălan, L., 2015. *Statistică economică.* Cluj: Editura Presa Universitara Clujeana.

Mahmood, Z., 2019. *The Internet of Things in the Industrial Sector* [e-book], Switzerland: Springer Nature. Available at: <https://www.springer.com/gp/book/9783030248918> [Accessed 21 October 2020].

Marr, B., 2020. *5 technology trends for 2021*. [online], Available at: <https://www.forbes.com/?sh=2a2343ed2254.> [Accessed 14 September 2020].

Mohamad Noor, M., Hassan, W.H., 2019. Current research on Internet of Things (IoT) security: A survey. *Computer Networks,* 148, pp.283-294.

Nagy, J., Oláh, J., Erdei, E., Máté, D., Popp, J., 2018. The Role and Impact of Industry 4.0 and the Internet of Things on the Business Strategy of the Value Chain –The Case of Hungary. *Sustainability,* 10, pp.34-91.

Neilkar T.S., Ankit Bhurane, A., Ashwin Kothari, A., 2020. Battery-less internet of things – A survey. *Computer Networks*, 180, pp.107-118.

Nizetic S., Solic P., Gonzalez-de-Artaza D.L., Patrono L., 2020. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Cleaner Production*, 274, pp.191-201.

Ozdemir, V.,2018. The Dark Side of the Moon: The Internet of Things, Industry 4.0, and The Quantified Planet OMICS. *A Journal of Integrative Biology*, 22(10), pp.12-17.

Qi, J., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 20(8), pp.2481-2501.

Sicaria, S., Rizzardia, A., Miorandib, D., Cappielloc, C., 2016. A secure and quality-aware prototypical architecture for the Internet of Things. *Information Systems,* 58, pp.43-55.

Szenteși, S.G., Cîrnațu, D., Szenteși, E., 2018. The impact of digitalization of communication in the way we understand the communication of the Risks Related to Diseases in the present and future. *4e Colloque International Comsymbol Journal Essachess,* 4, pp.178-190.

Tang, G., Shi, Q., Zhang, Z., He, T., Sun, Z., Lee, C., 2021. Hybridized wearable patch as a multi-parameter and multi-functional human-machine. *Nano Energy*, 81, pp.136-140.

Wang, C., Gill, Ch., Lu, Ch., 2020. Adaptive Data Replication in Real-Time Reliable Edge Computing for Internet of Things. *2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp.123-145.

Wu, Yi., Wu, Ya., Guerrero, J.M., Vasquez, J.C., 2021. Digitalization and decentralization driving transactive energy Internet: Key technologies and infrastructures, *International Journal of Electrical Power & Energy Systems*, 126(A), pp.127-139.

Annex no. 1. Data regarding companies and respondents

Data regarding the organisation							Data regarding the respondents			
No. crt	Code CAEN	Activity object	Area of activity	Locality	Company size	No.of employees	Level of studies	Profession	Position in the company	Gender
1	2932	Manufacture of other parts and accessories for vehicles and engines for vehicles	Production	Giarmata	big	460	Bachelor	Economist	Operations Manager	M
2	5221	Annex services activities for terrestrial transportation	Services	Codlea	small	3	Bachelor	Engineer	General Manager	M
3	1623	Manufacture of carpentry and carpentry elements for construction	Production	Arad	big	295	Master	Economist	Fiancial Director	F
4	2620	Production of electronic assemblies/equipment	Production	Ghimbav	big	674	Bachelor	Engineer	Production Director	M
5	2562	General mechanical operations	Production	Timisoara	medium	165	Master	Engineer	General Manager	M
6	2361	Manufacture of concrete construction products	Production	Arad	medium	111	Bachelor	Economist	Economic Director	F
7	3821	Treatment and disposal of non-hazardous waste	Services	Arad	medium	144	B	Engineer	Operations Manager	M
8	4651	IT systems integrator	Services	Buzau	small	9	Bachelor	System Engineer	Technical Manager	M
9	6209	Soft development and production	Services	Arges Bucureşti	medium	29	Bachelor	Economist	Project Manager	M
10	2932	Manufacture of other parts and accessories for motor vehicles and engines for vehicles	Production	Braşov Reşita Timisoara Sf. Gheorghe Iasi Preimer	big	8581	Bachelor	Economist	Project Manager	M
11	6202	Automation for smart buildings	Production	Arad	small	4	Bachelor	Computer engineer	Administrator	M
12	3250	Manufacture of dental medical devices, equipment and instruments	Producţie	Arad	big	721	Master	Linguist	Logistics Director	F
13	2612	Production of electronic devices and plates, including IoT devices for other companies	Production	Arad	big	644	Bachelor	Computer engineer	General Director	M
14	7311	Production advertising materials	Production	Arad	small	22	Bachelor	Economist	Administrator	M
15	2931	Fabricarea de echipamente electrice şi electronice pentru autovehicule şi pentru motoare de autovehicule	Production	Arad	big	3311	Master	Computer techni	IT Manager	M
16	2611	Manufacturing electronic subassemblies	Production	Lipova	big	396	Bachelor	Lawyer	Human Resources Manager	F
17	2932	Manufacture of other parts and accessories for motor vehicles and engines for vehicles	Production	Zimandu Nou	big	1207	Bachelor	Engineer	General Director	M
18	6120	Telecomunications solutions provider	Services	Timişoara	big	1861	Bachelor	Engineer	Sales Director	M
19	1419	Manufacture of other articles of clothing and accessories	Production	Arad	medium	64	Bachelor	Engineer	Administrator	F
20	4941	Road freight transport	Services	Arad	medium	221	Bachelor	Economist	Financial Director	F
21	6209	Other information technology service activities	Production	Braşov	small	3	Bachelor	Journalist	Technical Director	M
22	2229	Injection plastic parts	Production	Oradea	small	55	Master	Electronic engineer	Administrator	M
23	1431	Manufacture by knitting or crocheting of stockings and gallantry articles	Production	Buruienesti-Neamt	medium	50	Master	Navigator	Administartor	M
24	4941	Domestic and international freight transport	Services	Arad	big	366	Bachelor	Engineer	Administrator	M
25	2732	Fabrication of other electrical and electronic wires and cables	Production	Arad	medium	341	Master	IT	IT Manager	M