https://doi.org/10.48009/4_iis_2020_26-35

THE INTERNET OF THINGS CHALLENGES – COUNTRY AND INDUSTRY ANALYSES

Magdalena Mądra-Sawicka, Warsaw University of Life Sciences – SGGW, Poland, magdalena_madra@sggw.edu.pl
Joanna Paliszkiewicz, Warsaw University of Life Sciences – SGGW, Poland, joanna_paliszkiewicz@sggw.edu.pl
Salome Svanadze, Illia State University,Georgia, salome.svanadze.1@iliauni.edu.ge
Ardak Nassir, L.N. Gumilyov Eurasian National University, Kazakhstan askak88@mail.ru
Andrei Stefan Nestian, Alexandru Ioan Cuza University, Iași, Romania, nestian@uaic.ro
Meelis Kitsing, Estonian Business School, Estonia, Meelis.Kitsing@ebs.ee

ABSTRACT

The Internet of Things is recognized as one of the most important emerging technology. It is is the connection of physical objects that collect and transfer data from one object to another. The Internet of Things is expected to change the day to day companies' operation and influence economic development. The purpose of this article is to investigate the differences in the IoT challenges assessment across companies in international and industry comparison. The two research questions are presented: to identify IoT crucial challenges across countries and sector differences and to assess the diversity of the IoT challenges between the distinguished country groups. The article presents the theoretical issues concerning the IoT challenges. Next, the research results are presented. In the end, research findings, limitations, and implications for future research are discussed.

Keywords: Internet of Things (IoT), IoT challenges, developing technology

INTRODUCTION

The Internet of Things (IoT) is regarded as one of the most developing technologies of last years and has caught the attention of the academy and business (Tarabasz, 2016; Balaji and Roy, 2017; Fazal et al., 2017; Lee et al., 2018; Amiruddin, et al., 2019; Songsom, 2019; Kassab, et al., 2020).

Many definitions of the IoT are available in the literature (Nord et al., 2019). According to Mattern and Floerkemeier (2010, p. 242), IoT's are the items connected to the virtual world where they are "controlled remotely and can act as physical access points to the Internet services". With a different perspective, Amiruddin et al. (2019, p. 248) picturing the IoT as "an internetworking of physical objects such as sensors, actuators, personal computers, software, intelligent devices, automobile, and network connectivity that enable them to collect and exchange data without human intervention". Dorsemaine et al., (2015) present another view: IoT is a group of infrastructures interconnecting connected objects and allowing their management, data mining and access to the data they generate. A similar definition is presented by Gubbi et al. (2013), they described the IoT as the interconnection of devices that provides the possibility to exchange information across platforms through a unified framework. The popularity and development of IoT have led to extensive interconnections between people, services, sensors, and objects. IoT has been applied in many objects such as smart homes, logistics, cities, healthcare, energy management.

Internet of Things requires a more in-depth overview to map its application domains in different countries, industries and challenges. There have been several comprehensive scientific projects that study various aspects of IoT. However, there is a need to discuss specifically and intensely about the IoT challenges approach in different countries and industries. It has not been described in the literature yet.

The purpose of the study is to investigate the differences in the IoT challenges approach of companies in international and industry comparison. Therefore, we sought to answer the following research question (RQ):
RQ1: identify IoT crucial challenges across countries and sector differences
RQ2: assess the diversity of the IoT challenges between the distinguished country groups.

The first part of the article presents the theoretical issues concerning IoT challenges. In the second part, the research methodology of the study is described, and the results of the analysis are presented. Discussion, conclusions with limitations, and avenues for further research end the publication.

THE CHALLENGES OF THE INTERNET OF THINGS

With the development of the Internet of Things, we are moving towards a society where everything and everyone will be connected. IoT provides connectivity for anyone at any time and place to anything at any time and place (Zheng et al., 2011). There are many challenges related to IoT, for example, access control, authentication, cooperation, integration among technologies, lack of international norms and standards, policy enforcement, networking challenges, security, privacy, resources, return on investment, security, too few best practices and trust. We presented in the literature review only the most often investigated challenges by researchers.

Access control and authentication are the main issues related to the security of IoT devices. Only authenticated and authorized users should be able to access the system (Kavianpour et al., 2019). Authentication factors are ownership (smart cards and smartphones), knowledge (passwords), and biometrics (fingerprint) (Choi, et al., 2014). The IoT systems consist of a multitude of devices and sensors that communicate with each other and transfer a massive amount of data over the Internet (Hao, et al., 2015). It gives rise to complex issues of integration and cooperation among technologies. Especially, support cooperation and integration of many devices with different memory, processing, storage power, and bandwidth (Pereira and Aguiar, 2014); Given the increased communication of IoT technology, there are increased security-related concerns. Devices collect many types of data, but it should be clear who owns the data and where the data go. There is a need to establish international norms and standards. In this area, the governments should collaborate with businesses to harmonize compliance requirements and create an appropriate policy on the international level (Tikk-Ringas, 2016). With the coming of the massive IoT era (Hsing-Chung, 2019), the networking challenges appear, which include the quality of service, reliability, cost, energy consumption, availability, and service time (Huo and Wang, 2016). Essential issues of IoT that require attention are the security and privacy (Weber, 2010; Nord et al., 2019). Privacy includes the ability to control what happens with this information and the concealment of personal information. Another challenge is related to the availability of experts in this area or implementing appropriate training and education to help to develop skills among employees. Return on Investment (RoI) is another issue. It can be defined is a key metric to assess the performance of an investment strategy and compare it to alternatives (Mobley, 2002; Feibel, 2003). For effective calculation of the RoI of IoT project, it is imperative to understand which savings can be attributed to its implementation as well as how to determine the size of investment required (Houston et al., 2017). It is also crucial to understand and document existing best practices in IoT businesses to help further development. The last issue is trust in IoT, which creates the foundation to use this technology. Trust helps people overcome perceptions of uncertainty and risk and engages in user acceptance and consumption on IoT services and applications. Trust management plays an important role in Internet of Things for reliable data mining, qualified services with context-awareness, and enhanced information security and user privacy (Yan et al., 2014).

The last few years have seen an explosion in the Internet of Things devices and connected products. Businesses are taking advantage of IoT to increase productivity and efficiency. Therefore, it is important to take into consideration the described challenges when developing and introducing IoT devices.

METHODS

Instrument

The instrument survey used for this study consisted of four parts concerning IoT: external application usage, internal application usage, IoT benefits, and IoT challenges. The research concerns only the case of IoT challenges. Investigated in a questionnaire IoT challenges consisted of 14 areas, i.e., access control, authentication, cooperation, integration among technologies, lack of international norms and standards, mobile security, networking challenges, policy enforcement, privacy, resources (skilled personnel), return on investment, security, too few best practices and trust. A five-point Likert-type scale: 1 – extremely top priority, 2 – a top priority, 3 – neutral, 4 – low priority, 5 – an extremely low priority was used for the answers.

Sample and procedure

The study was conducted in 2019. Data were collected electronically among six countries: Romania, Poland, Estonia, Kazakhstan, Georgia, and the US. A sample of the study includes a total of 483 responses (195 from Romania, 102 from Poland, 8 from Estonia, 119 from Kazakhstan, 14 from Georgia, and 45 from the US). The study was conducted through the cooperation of enterprises with universities located in selected countries. The survey was translated into the native language and administered on-line from the USA. Participation in completing the survey was entirely voluntary, and the companies were assured confidentiality and anonymity. The choice of the sample was dictated by taking into account trends in IoT challenges both in the group of emerging markets compared to the developed economy of the US.

Data analysis

Descriptive statistics in the first stage were used to realize the identify IoT challenges that companies faced. The analysis includes country and industry perspective. The second stage concerned the assessment of the diversity of the IoT challenges between the distinguished country groups. The Kruskal-Wallis ANOVA test was carried out with rankings according to the ordinal scale. The purpose of identifying diversity between the company groups was to verify the following hypotheses:
H0: All enterprises within the country division had similar IoT challenges assessment.
H1: Not all enterprises within the country division had similar IoT challenges assessment.
To verify the theses, an assessment based on multiple (two-sided) comparisons for given groups of countries was made. The study includes following IoT challenges for companies: Access Control, Authentication, Cooperation, Integration among Technologies, Lack of International Norms and Standards, Mobile Security, Networking Challenges, Policy Enforcement, Privacy, Resources, Return on Investment, Security, Too Few Best Practices and Trust.

RESEARCH RESULTS

The enterprises represent five areas of operation (See Figure 1). The largest group of companies in total was classified as service companies (42%), the second one was retail companies (17%), and the third was manufacturing (16%). The service companies were dominating the investigated sample in each country apart from Kazakhstan, where the government sector represented 34% of companies (11% in the total sample). In the case of Estonia and Georgia sample retail sector was not investigated.

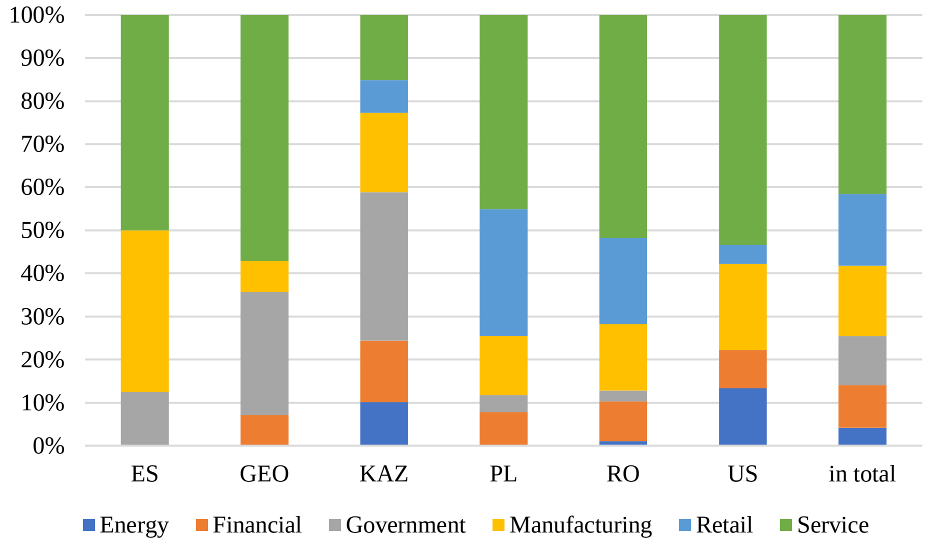

Figure 1: Companies field of operation - the country division
Note: ES – Estonia, GEO – Georgia, KAZ – Kazakhstan, PL – Poland, RO – Romania, US – United States.

Figure 2 presents the distribution of employment in the surveyed enterprises in the country division. The highest share in the examined group of companies noticed for enterprises employing from 1 to 250 employees; the percentage of these entities constituted 53%. The highest share of companies hiring more than 1000 employees was representing the US sample (62% of investigated companies).

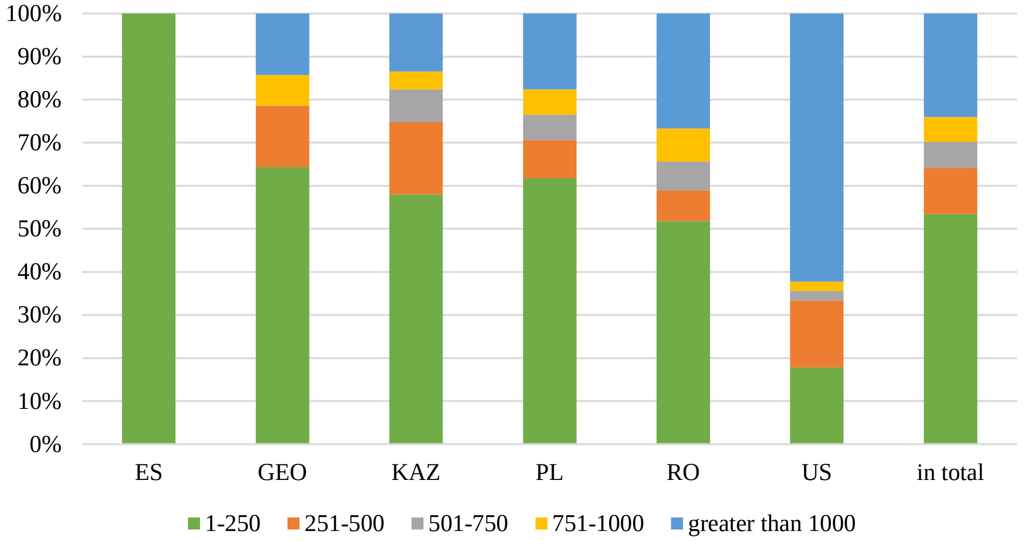

Figure 2: Number of employees within surveyed companies - the country division
Note: ES – Estonia, GEO – Georgia, KAZ – Kazakhstan, PL – Poland, RO – Romania, US – United States.

Among investigated companies, 64.2% were using IoT, and the highest share of these companies notice in the US (88.9%) and Poland (88.2%). Companies that are before IoT system implementation in the second stage of the questionnaire evaluated the importance of the challenges that they need to face to introduce it (Figure 3).

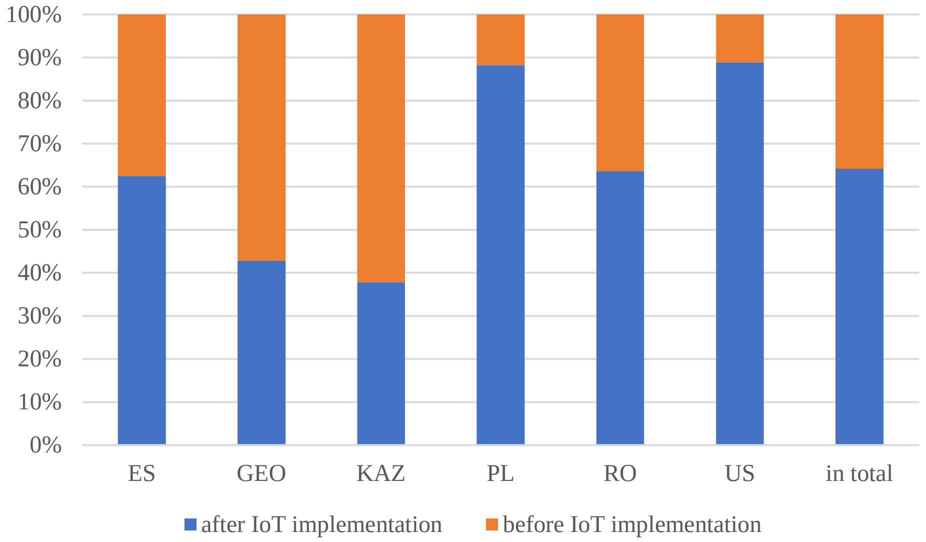

Figure 3: IoT implementation in the company
Note: ES – Estonia, GEO – Georgia, KAZ – Kazakhstan, PL – Poland, RO – Romania, US – United States.

IoT average challenges ranking assessment is presented in Figure 4. The top rank challenges were: Mobile Security, Privacy, and Security. The lowest ranks observe for Too Few Best Practices, which could be related to individuals/specific company operations and knowledge sharing issues. For three top rank challenges, prepared the industry assessment for most representative sectors in a sample: service, retail, and manufacturing (Table 1).

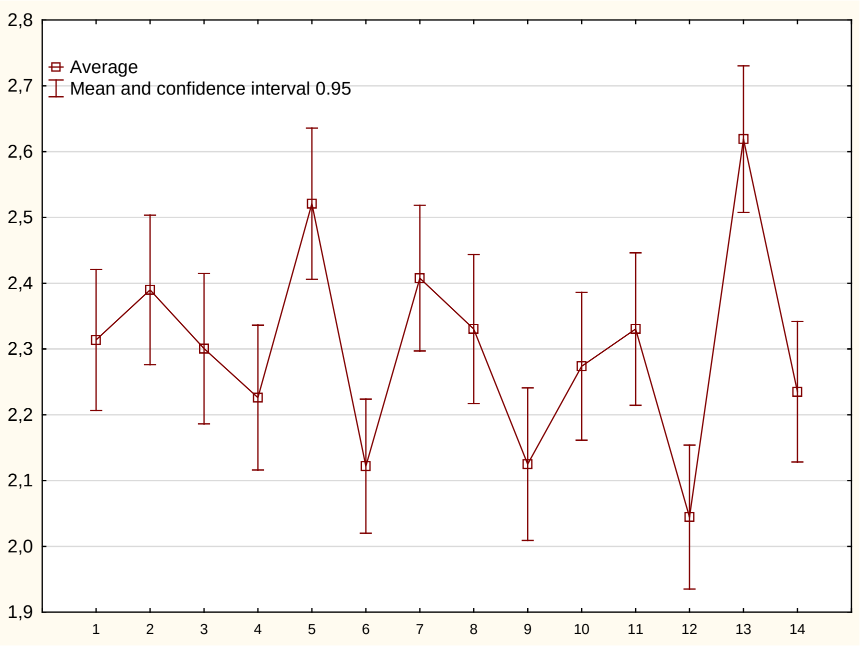

Figure 4: Average IoT challenges rank with a confidence interval

Note: X-axis - 1 – Access Control, 2 – Authentication, 3 – Cooperation, 4 – Integration among Technologies, 5 – Lack of International Norms and Standards, 6 – Mobile Security, 7 – Networking Challenges, 8 – Policy Enforcement, 9 – Privacy, 10 – Resources (skilled personnel), 11 – Return on Investment, 12 – Security, 13 – Too Few Best Practices and 14 – Trust.
Y-axis - Rank: 1 – extremely top challenge, 2 – top challenge, 3 – neutral, 4 – low challenge, 5 – extremely low challenge.

In the manufacturing sector, the security challenges of IoT were assessed as the most demanding (2.08); however, the privacy noticed a higher standard deviation (51.76%) (see Table 1). In the case of the retail sector, the privacy noticed the top rank (2.20) and for security recorded the highest level of variation (50.04%). The most represented services sector noted the most top assessment of challenges faced by entrepreneurs in the field of privacy and security (1.97).

Table 1: The highest-ranked IoT challenges assessment across sector comparison

		N	Average	Median	Standard deviation	Coefficient of variation
Manufacturing	Mobile Security	48	2.208333	2.000000	0.849489	38.46742
	Privacy	48	2.145833	2.000000	1.110675	51.75962
	Security	48	2.083333	2.000000	0.895220	42.97055
Retail	Mobile Security	58	2.293103	2.000000	0.936747	40.85063
	Privacy	58	2.120690	2.000000	0.992562	46.80372
	Security	58	2.206897	2.000000	1.104355	50.04110
Service	Mobile Security	132	2.030303	2.000000	0.964558	47.50809
	Privacy	132	1.977273	2.000000	0.976564	49.38946
	Security	132	1.977273	2.000000	0.976564	49.38946

The list of challenges faced by companies in the country division when implementing and utilizing the IoT is presented in Table 2. All unique challenges in IoT noticed the assessment on an average level lower than 3.0. It explains that all challenges were assessed as "extremely high" or "high." The highest average challenged rank was noticed for security (2.04), which was crucial special in the case of polish investigated companies (1.79).

Table 2: Average IoT challenges assessment - the country division

Detailed	ES	GEO	KAZ	PL	RO	US	Total
1. Access Control	3.00	2.43	2.36	2.00	2.46	2.50	2.31
2. Authentication	-	2.43	2.58	1.94	2.69	2.33	2.39
3. Cooperation	2.80	2.57	2.15	2.17	2.38	2.60	2.30
4. Integration among Technologies	3.00	2.29	2.31	1.94	2.24	2.60	2.23
5. Lack of International Norms and Standards	3.20	2.29	2.25	2.63	2.54	2.74	2.52
6. Mobile Security	2.20	3.14	2.30	2.02	1.97	2.19	2.12
7. Networking Challenges	3.20	3.00	2.38	2.25	2.48	2.45	2.41
8. Policy Enforcement	4.00	2.71	2.17	2.15	2.46	2.50	2.33
9. Privacy	3.60	3.29	2.43	1.80	1.95	2.33	2.13
10. Resources	2.80	2.71	2.42	1.85	2.28	2.83	2.27
11. Return on Investment	2.60	2.14	2.33	2.04	2.42	2.79	2.33
12. Security	2.20	2.57	2.13	1.79	2.15	2.12	2.04
13. Too Few Best Practices	2.40	2.57	2.40	2.94	2.48	2.64	2.62
14. Trust	2.80	2.29	2.18	2.03	2.39	2.38	2.24

Note 1 – extremely top challenge, 2 – top challenge, 3 – neutral, 4 – low challenge, 5 – extremely low challenge. ES – Estonia, GEO – Georgia, KAZ – Kazakhstan, PL – Poland, RO – Romania, US – United States.

The rank of the list of challenges faced by companies in the sector division in implementing and utilizing the IoT is presented in Table 3. In the case of the Energy sector, the top challenges of IoT were selected Security (1.59) and Mobile Security (1.71). These ranks were the highest in all investigated IoT challenges across listed sectors. In the finance sector, the Resources (1.92), Security (1.92), and Authentication (1.95) were asses as the main demanding. In manufacturing companies, the most challenging was Security issues (2.08) and privacy (2.15); similarly, the Retail companies ranked these challenges as follows 2.21 and 2.12. However, for manufacturing companies, security was more important, while for retail, it was privacy. In the case of service companies, the privacy and security issues noticed an equal rank with the highest challenging assessment in IoT implementation.

Table 3: Average IoT challenges assessment - the sector division

Detailed	Energy	Financial	Government	Manufacturing	Retail	Service
1. Access Control	2.06	2.08	2.52	2.33	2.34	2.33
2. Authentication	2.11	1.95	2.65	2.53	2.48	2.38
3. Cooperation	2.24	2.11	2.12	2.27	2.53	2.33
4. Integration among Technologies	2.47	1.92	2.35	2.17	2.22	2.27
5. Lack of International Norms and Standards	2.12	2.63	2.33	2.44	2.81	2.51
6. Mobile Security	1.71	2.00	2.35	2.21	2.29	2.03

Table 3: Average IoT challenges assessment - the sector division

Detailed	Energy	Financial	Government	Manufacturing	Retail	Service
7. Networking Challenges	2.12	2.16	2.56	2.44	2.48	2.42
8. Policy Enforcement	1.94	2.18	2.42	2.33	2.43	2.35
9. Privacy	2.35	2.11	2.49	2.15	2.12	1.98
10. Resources	2.59	1.92	2.42	2.38	2.31	2.23
11. Return on Investment	2.65	2.18	2.37	2.42	2.33	2.29
12. Security	1.59	1.92	2.28	2.08	2.21	1.98
13. Too Few Best Practices	2.06	2.55	2.42	2.71	2.88	2.63
14. Trust	2.18	2.24	2.19	2.33	2.33	2.18

Note 1 – extremely top challenge, 2 – top challenge, 3 – neutral, 4 – low challenge, 5 – extremely low challenge.

Table 4 presents the non-parametric test results of Anova Kruskal-Wallis by including only the significant differences among investigated IoT challenges that faced companies among investigated countries. The significant differences among the listed IoT challenges were noticed mostly in countries with the biggest sample. The following IoT challenges were equally assessed among investigated countries: Cooperation, Integration among Technologies, Lack of International Norms and Standards, Networking Challenges, Security, and Trust. The country specification noticed in case of privacy issues for which the significant differences of these IoT challenges assessment notice for Poland vs. Estonia and Kazakhstan and Romania vs. Estonia and Kazakhstan.

In case of attitude to IoT challenges across emerging and developed economies recorded significant changes for Poland and the US in case of resources and returned on investment. The Authentication and Too Few Best Practices were perceived differently by Poland and differently by entities from Kazakhstan and Romania.

Table 4: Results of multiple two-sided comparisons – the country division

Detailed	**Significant differences**	**The P-value for multiple (two-sided) comparisons**
1. Access Control	Poland vs. Romania	.047022
2. Authentication	Poland vs. Kazakhstan Poland vs. Romania	.001271 .000044
3. Cooperation	-	-
4. Integration among Technologies	-	-
5. Lack of International Norms and Standards	-	-
6. Mobile Security	Poland vs. Romania	.035868
7. Networking Challenges	-	-
8. Policy Enforcement	Poland vs. Estonia 2vs 3	.015552 .015584
9. Privacy	Poland vs. Estonia Poland vs. Kazakhstan Estonia vs. Romania Kazakhstan vs. Romania	.010573 .001253 .024450 .020528
10. Resources	Poland vs. Kazakhstan Poland vs. US	.003548 .000144

Table 4: Results of multiple two-sided comparisons – the country division

Detailed	Significant differences	The P-value for multiple (two-sided) comparisons
11. Return on Investment	Poland vs. US	.031801
12. Security	-	-
13. Too Few Best Practices	Poland vs. Kazakhstan Poland vs. Romania	.006721 .019122
14. Trust	-	-

The Anova Kruskal-Wallis and multiple two-sided comparisons test in sector analyses could not be done due to not a balanced sample between industries that survey companies' representation.

DISCUSSION

Securing the IoT devices by creating a new mechanism for a new solution seems to be a fundamental matter in company assessment in-country and industry approach. The implication of this solution will be crucial for further IoT devices application and then technology development. Furthermore, the service industry ranks the privacy and securities issues as essential IoT challenges implementation. The security issues were important in every country and every investigated industry. It confirmed tendencies observed by Khan, Salah (2018), and security problems with wireless sensor networks, machine-to-machine, and cyber-physical systems. The stored data on different devices can be potential changes, modified, stoled. The high-level security issues, according to Khan and Salah (2018), concerns the IoT applications used for IoT access via web interfaces, mobile, cloud, or different platforms. It also covers the investigated in the study problem of privacy IoT challenge. Security issues in IoT open wearable devices usage were also assessed as crucial by Zhang et al. (2014) in case of a large data-sharing process that contains private information that should be secured. The results evidenced by Hossain et al. (2015) also noticed problems of surface attacks, the threat of IT model, and growing technology requirements. The requirements of security issues for the IoT have also underlined in Oh and Kim (2017) study in which the problem of IoT implementation concerns the dynamic environment of companies and resource constraints. These problems also relate to IoT elements like IoT network, cloud, potential users, services, and platform creating. IoT introduces opportunities for hackers; thus, IoT requires techniques, tools, and solutions (Yaqoob et al., 2019). So the further trend in IoT implementation should ensure confidentiality, authentication, access control, and integrity Razzaq et al. (2017). These attitudes to IoT challenges were confirmed by survey results from the international and industry perspective.

CONCLUSIONS

The purpose of this study was to investigate the differences in the IoT challenges evaluation of companies in international and industry viewpoint. Therefore, we sought to answer the following research question (RQ):
RQ1: identify IoT crucial challenges across countries and sector differences
RQ2: assess the diversity of the IoT challenges between the distinguished country groups.
The crucial challenge identified across countries was security issues. It did not differ in country analyses and always noticed one of the highest ranks in industry comparison. The highest rank of IoT implementation challenges like mobile security, privacy, and security noticed in the manufacturing, service and retail industry. In the case of country division, the privacy issues were diverse across Poland vs. Estonia, Poland vs. Kazahstan, Estonia vs. Romania, and Kazahstan vs. Romania. It could be determined by the unbalanced sample of industry representatives in each country but is also relates to security IoT challenges. Due to the unbalanced industry sample, it noticed insignificant results that were not presented in the study.
The limitation of the study concerns the unbalanced sample of companies surveyed by industry and country division. Based on the results presented, no conclusions can be conveyed for the entire population. The results present directions for assessing the IoT challenges that companies faced among different countries and industries.

FUTURE RESEARCH

Further research is needed in this area by using more representative samples and increasing the number of countries in the study. In addition, mixed methods can be used to explore processes in a more detailed way for understanding the risks and opportunities in the diffusion of IoT. Future research on the IoT can also benefit by linking it conceptually to the scholarship on digital platforms. The nature of IoT development depends on what kind of platform infrastructure will emerge. Will centralized end-to-end platforms dominate in the IoT diffusion or will diverse platforms co-exist and complement each other in the digital ecosystems.

REFERENCES

Amiruddin, A., Ratna, A. A. P., & Sari, R. F. (2019). Systematic review of Internet of things security. *International Journal of Communication Networks and Information Security, 11*(2), 248-255.

Balaji, M. S., & Roy, S. K. (2017). Value co-creation with Internet of Things technology in the retail industry. *Journal of Marketing Management, 33*(1-2), 7-31.

Choi, Y., Nam, J. Lee, D., Kim, J., Jung, J., & Won, D. (2014). Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics, *The Scientific World Journal*, Article ID 281305.

Dorsemaine, B., Gaulier, J. P., Wary J. P., Kheir, N. & Urien, P. (2015). *Internet of Things: A Definition & Taxonomy*. 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK.

Fazal, K., Shehzad, H., Tasneem, A., Dawood, A., & Ahmed, Z. (2017). A systematic literature review on the security challenges of Internet of things and their classification. *International Journal of Technology and Research, 5*(2), 40-48.

Feibel, B.J. *Investment Performance Measurement*; John Wiley & Sons: Hoboken, NJ USA, 2003.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami. M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems 29*(7), 1645-1660.

Hao, Q., Zhang, F., Liu, Z., & Qin, L. (2015). Design of chemical industrial park integrated information management platform based on cloud computing and IoT (the Internet of Things) technologies. *International Journal of Smart Home, 9*(4), 35-46.

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the Internet of things. In *2015 IEEE World Congress on Services*, 21-28.

Houston, C., Gooberman-Hill, S., Mathie, R., Kennedy, A., Li, Y., & Baiz, P. (2017). Case study for the return on investment of internet of things using agent-based modelling and data science. *Systems, 5*(1).

Hsing-Chung, C. (2019). Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application. *Mobile Networks and Applications, 24*(3), 839-852.

Huo, L., & Wang, Z. (2016). Service composition instantiation based on cross-modified artificial Bee Colony algorithm. *China Communication, 13*(10), 233-244.

Kassab, M., DeFranco, J., & Laplante, P. (2020). A systematic literature review on Internet of things in education: Benefits and challenges. *Journal of Computer Assisted Learning, 36*(2), 115-127.

Kavianpour, S., Shanmugam, B., Azam, S., Zamani, M., Samy, G. N., & De Boer, F. (2019). A systematic literature review of authentication in Internet of things for heterogeneous devices. *Journal of Computer Networks and Communications,* Article ID 5747136, Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

Lee, C. K. M., Lv, Y., Ng, K. K. H., Ho, W., & Choy, K. L. (2018). Design and application of Internet of Things-based warehouse management system for smart logistics. *International Journal of Production Research*, *56*(8), 2753-2768.

Mattern, F. & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. In K. Sachs, I. Petrov, P. Guerrero (Eds). *From Active Data Management to Event-Based Systems and More*. Volume 6462 (pp. 242-259). Berlin/Heidelberg, Germany: Springer.

Mobley, R.K. *An Introduction to Predictive Maintenance*; Butterworth-Heinemann: Woburn, MA, USA, 2002.

Nord, J. H., Koohang, A. & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications, 133,* 97-108.

Oh, S. R., & Kim, Y. G. (2017). Security requirements analysis for the IoT. In *2017 IEEE International Conference on Platform Technology and Service (PlatCon)*, pp. 1-6.

Pereira, C., Aguiar, A. (2014). Towards efficient mobile M2M communications: survey and open challenges. *Sensors, 14*(10), 19582-19608.

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): a comprehensive study. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(6), 383-388.

Songsom, N., Nilsook, P., & Wannapiroon, P. (2019). The student relationship management system process via the Internet of things. *TEM Journal, 8*(4), 1426-1432.

Tarabasz, A. (2016). The Internet of Things – digital revolution in offline market. Opportunity or threat? *Handel Wewnetrzny, 363*, 325-337.

Tikk-Ringas, E. (2016). International cyber norms dialogue as an exercise of normative power. *Georgetown Journal of International Affairs, 17*(3), 47-59.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26,* 23-30.

Yan, Z., Zhang, P., Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Applications, 42*, 120-134.

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, *92*, 265-275.

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. In *2014 IEEE 7th international conference on service-oriented computing and applications,* 230-234.

Zheng, J., Simplot-Ryl, D., Bisdikian, C., & Mouftah, H. (2011). The Internet of Things. *IEEE Communications Magazine, 49*(11), 30-31.