THE CHALLENGES OF INTERNET OF THINGS ADOPTION IN DEVELOPING COUNTRIES: AN OVERVIEW BASED ON THE TECHNICAL CONTEXT

Ayman Altameem

Department of Computer and Engineering Sciences, College of Applied Studies and Community Services, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

The Internet of Things (IoT) has the potential to change the way we engage with our environments. Its prevalence has spread to various areas of industrial and manufacturing systems in addition to other sectors. However, many organizations are finding it increasingly difficult to navigate IoT. To unleash its full potential and create real economic value, it is essential to learn about the obstacles to IoT delivery. There is high potential for IoT implementation and usage in developing countries, and major barriers must be addressed for IoT delivery. This paper explores the challenges that impact the adoption of IoT in developing countries based on the technical context. It also presents a general conclusion in the form of recommendations to capture the maximum benefits of IoT adoption.

KEYWORDS

Internet of Things adoption, Obstacles of IoT in developing countries, IoT Technical Context.

1. INTRODUCTION

IoT offers tremendous potential to transform the globe by linking devices in large interoperable systems managed by analytics and software [1]. IoT is one of the most significant emerging technologies [2], [3]. It allows anyone in any location to connect to anything at any point in time using a device [4]. IoT has been recognized for its impacts on various sectors, including construction and manufacturing, healthcare, logistics, oil and gas, agriculture, and transportation. IoT system has the ability to empower all industries to change from conventional business models to new revenue streams [54]. Figure 1 illustrates the global IoT market share as determined by Fortune Business Insights [6], which divided the market into banking, financial services, and insurance (BFSI), transportation, healthcare, information technology (IT), telecom, manufacturing, government, agriculture, retail, sustainable energy, and other sectors. Accordingly, healthcare and manufacturing were anticipated to have the largest IoT market share in 2021 [6].

David C. Wyld et al. (Eds): CST, NLMLT, DMS, CLBD, ITCS, VLSIE - 2022
pp. 111-118, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.121910

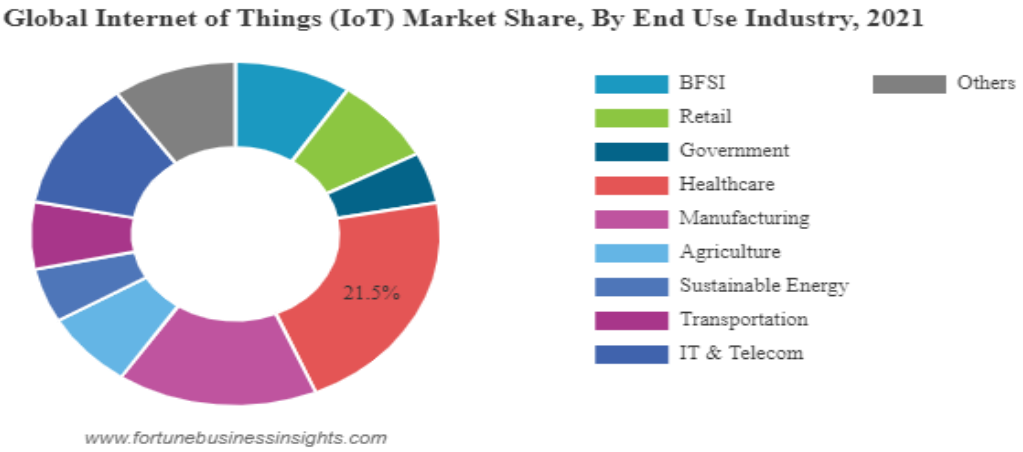

Figure 1. Global IoT market share [6]

The significant influence of IoT on the Internet and global economy is remarkable. It is anticipated that by 2025, there will be close to 100 billion linked IoT devices [7] and a world economic impact in excess of $11 trillion [8], which would equate to around 11% of the global economy based on the World Bank's projection of $99.5 trillion per year in global GDP in 2025 [8]. Figure 2 shows the anticipated rise in the enterprise IoT market [10], which rose by more than 22% between 2020 and 2021 to $157.9 billion. IoT Analytics estimates that the IoT market share will rise at a compound annual growth rate (CAGR) of 22.0% between 2022 and 2027 to eventually total $525 billion.

Customers will capture the utmost of the advantages. [8] showed that the users of IoT, including consumers, businesses, and other organizations, might be able to capitalize on 90% of the value that IoT applications produce. Accordingly, for example, the value of enhancing the health of chronic disease patients over remote monitoring will possibly be approximately $1.1 trillion each year in 2025 [8].

Organizations are utilizing IoT technology to increase efficiency and effectiveness [11], [44] in addition to enhancing decision-making [46], [47] and increasing the value of the business [39], [40], [47], [48]. The active nature and rapid changes in IoT have revealed obstacles and issues that might stand in the way of allowing users to capture its advantages [12]. Thus, the process of understanding the major challenges that influence the adoption of IoT is a very important endeavor.

A further in-depth overview is needed to map the obstacles associated with the implementation and adoption of IoT in developing countries. Experts estimate that by 2025, 40% of the economic value added from IoT will be generated in the developing world [13].

The aim of this paper is to explore the major challenges to implementing IoT in developing countries based on the technical context. This paper provides an inclusive outline to aid in further research in this field. Tackling these challenges will help organization leaders and IT professionals in developing countries take an efficient course of action during IoT delivery.

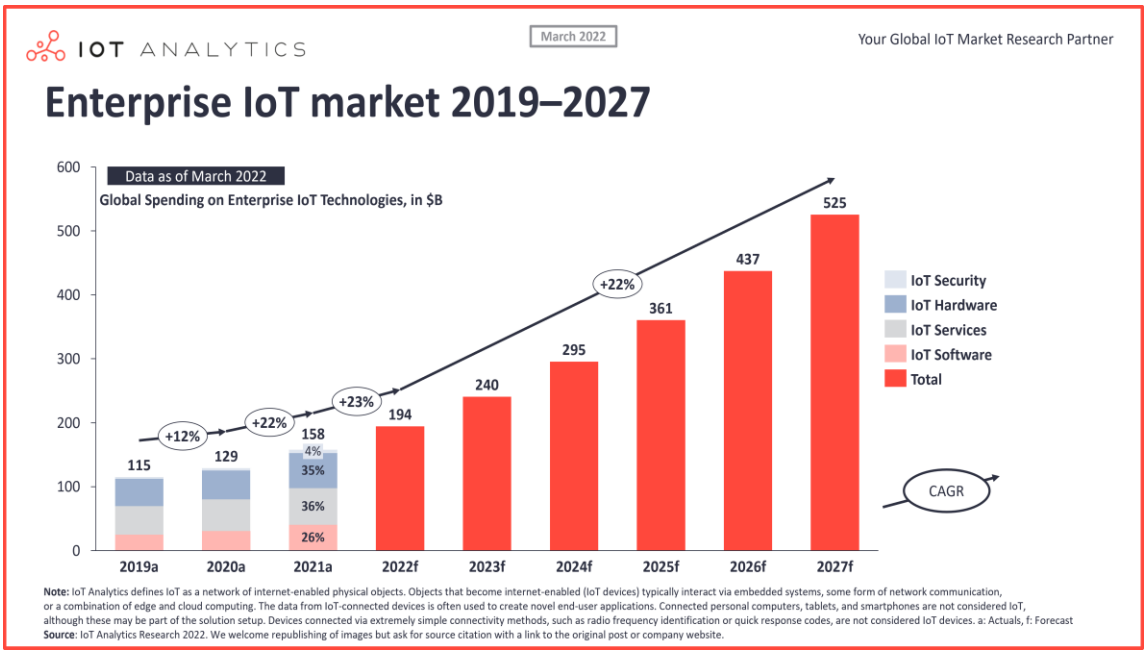

Figure. 2. Growth in the enterprise IoT market [10]

2. INTERNET OF THINGS (IOT)

Researchers have offered several definitions of IoT [12]. [14] defined it as a network of devices linked with electronics, software, sensors, and network connectivity. [15] viewed 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." According to [16], IoT is a network of connected devices that are uniquely addressable based on standard communication protocols. [17] described IoT as a technology that enables individuals and things to be linked at any place and anytime, linking any service with anyone, and ideally using any path or network. Furthermore, [49] defined IoT as "a network that connects an ordinary physical object with an identifiable address to provide intelligent services." According to the Gartner Group, IoT "is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" [18].

3. CHALLENGES OF IOT

IoT has been recognized as an innovative technology, and its development has attracted great interest from many sectors worldwide [19]. Despite the technology's many potential benefits, including improving our quality of life [50], organizations in developing countries have encountered several obstacles to IoT adoption. Studies on IoT have addressed the following challenges based on the technical context: access control [20], [21], security [12],[24]–[29], [34],[36],[38], privacy [12], [27], [30]–[34],[36], IoT infrastructure [13], [35], [37], energy requirement [36], [37], [45], IoT expertise [13], [37], compatibility [31], [37], complexity [31], [34], [44], and connectivity [41]–[43]. These IoT challenges are illustrated in Figure 3.

3.1. Security and Privacy

Many researchers have emphasized security and privacy as major challenges to IoT delivery. [9] pointed out that IoT presents opportunities for hackers and has been associated with new security risks that application developers and device manufacturers cannot predict [55]. There are many threats that can impact IoT entities, such as attacks that target various communication channels, identity fabrication, denial of service, and physical threats [56]. End-user privacy can be threatened due to their restricted control and options over the collection, retention, and distribution of their data [55].

3.2. IT Infrastructure

The flexibility of IT infrastructure allows organization leaders to be the most advantaged by an IT system, since it can react to new developments more efficiently [57]. The lack of IT infrastructure could put countries at risk of being left behind in economic terms [58]. IT infrastructure is one of the IoT requirements. Many researchers [59] have noted that organizations could have problems adopting IoT systems due to their lack of IT infrastructure.

3.3. Power Requirement

In addition, reliable power resources are vital to powering IoT in many developing countries [45]. For most objects, energy is crucial. Sometimes, a lack of energy can even limit the lifespan of an object [51]. A stable and reliable power supply is vital to the enabling of these systems, as it is necessary for constant operation over a period of several months to years [52].

3.4. Compatibility

Several researchers have recognized the importance of compatibility in IoT adoption [31], [37]. In the prediction of communication-oriented services, perceived compatibility has been recognized as an important issue in determining a user's adoption of such services [53].

3.5. Complexity

Complexity leads to greater difficulty in the deployment of IoT applications. [60] pointed out that "The complexity of an innovation may be determined by the breadth and depth of knowledge required, and it acts as a barrier to potential adopters of IS innovation." A simplified implementation mechanism and ease of use of the technology are essential to the successful adoption of IoT applications.

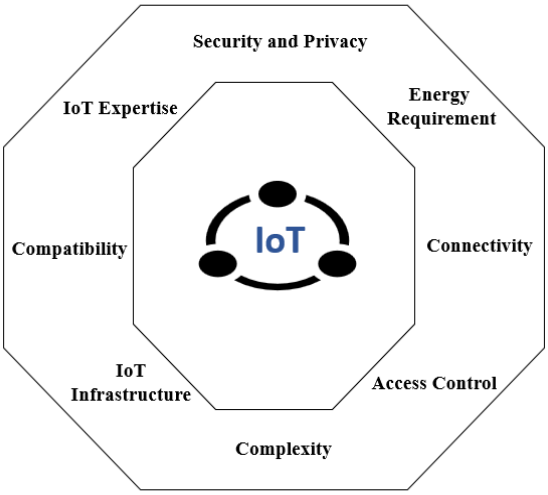

Figure. 3. Challenges of IoT

3.6. IoT Expertise

IT professionals are vital to the continuous development of IoT systems [61]. IoT systems require day-to-day maintenance and updates. Sufficient IT skills are required to increase its likelihood of implementation. [62] noted that the competition for IoT is the competition between technology and professionals.

3.7. Access Control

Access control is another aspect of great significance and sensitivity [63]. [5] basically defined access control systems as "software that is used to control access to files, records, etc." Access is permissible if it fulfils the rules related to the data [64].

3.8. Connectivity

In developing countries, one of the critical technological challenges is providing users with a sufficient Internet speed. IoT demands both scalability and reliable connectivity. Internet connectivity can be either an important barrier to or an enabler in the implementation of IoT.

Organizations must recognize and understand the complex realities inherent in the IoT adoption process. Only with such understanding can they develop the right methods, tools, and solutions to surmount these challenges and derive the maximum benefits from IoT.

4. CONCLUSIONS

As one of the most advanced emerging technologies, IoT is altering many industries and economies. It has a high potential to connect everyday objects to the Internet. Although IoT provides various benefits that improve our quality of life, there are major obstacles to its delivery that should be addressed. This paper examined the major IoT challenges in developing countries based on the technical context. This study presents an inclusive outline to aid further research in this area. This paper found that access control, security, privacy, IoT infrastructure, energy requirements, IoT expertise, compatibility, complexity, and connectivity are key barriers that impact IoT adoption. This paper can aid both practitioners and researchers. For practitioners, this

paper addressed the major obstacles that impact successful IoT adoption in developing countries. Organization leaders and IT professionals should take these obstacles into consideration so that they can take an efficient course of action when facilitating IoT delivery. As for researchers, this paper is a useful reference for further research in this area. Future studies can be conducted to validate these results by developing a tool and taking a survey of organizations.

REFERENCES

[1] Tektronix, (2016), A Guide To Building IoT Ready Devices, Available online: https://download.tek.com/document/37W_60226_2_IoT_eBook.pdf (accessed on 1 June 2022)

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

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

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

[5] Herold, R. (2007), Information Security Management Handbook (6th Ed.), Auerbach Publications, Canada, US.

[6] Fortune Business Insights, 2022, Internet of Things (IoT) Market, Available online: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307(accessed on 8 Sep 2022).

[7] "Global Connectivity Index." Huawei Technologies Co., Ltd., 2015, Available online: http://www.huawei.com/minisite/gci/en/index.html (accessed on 6 Sep 2015).

[8] Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon, "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, June 2015.

[9] 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.

[10] Wegner, P., 2022, Global IoT market size grew 22% in 2021 — these 16 factors affect the growth trajectory to 2027, IoT Analytics' Global IoT Enterprise Spending Dashboard, Available online: https://iot-analytics.com/iot-market-size/ (accessed on 8 Sep 2022).

[11] F. Restuccia, S. D. Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking," vol. 1, no. 1, pp. 1–14, 2018.

[12] Nord, J.H.; Koohang, A.; Paliszkiewicz, J, (2019), The IoT: Review and theoretical framework, Expert Syst. Appl, 133, 97–108.

[13] T. Scherf, (2016), Internet of Things—Hype or hope for developing countries? KfW Development Research, Available online: https://www.kfw-entwicklungsbank.de/PDF/DownloadCenter/PDF-Dokumente-Development-Research/Internet-of-Things-%E2%80%93-hype-or-hope-for-developing-countries.pdf(accessed on 5 Sep 2022).

[14] D. Mocrii, Y. Chen, P. Musilek, IoT-based smart homes: a review of system architecture, software, communications, privacy and security, Internet Things 1–2 (2018) 81–98, doi:10.1016/j.iot.2018.08.009.

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

[16] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw, 54 (2010) 2787–2805, doi:10.1016/j.comnet.2010.05.010

[17] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realizing the internet of things, Clust. Eur. Res. Proj. Internet Things Eur. Commision, (2010), doi:10.2759/26127

[18] Gartner Group, Internet of Things (IoT), Gartner Glossary, Available online: https://www.gartner.com/en/information-technology/glossary/internet-of-things (accessed on 19 Sep 2022).

[19] A. Al-fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, (2015), "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," vol. 17, no. January, pp. 2347–2376.
[20] Mishra, R., and Yadav, R. (2020), Access Control in IoT Networks: Analysis and Open Challenges, Available at SSRN 3563077.
[21] A. Ouaddah, H. Mousannif, A.A. Elkalam, A.A. Ouahman, (2017), Access control in the internet of things: big challenges and new opportunities, Comput. Netw., 112 (2017), Pages 237-262
[22] Pereira, C., Aguiar, A. (2014), Towards efficient mobile M2M communications: survey and open challenges, Sensors, 14(10), 19582-19608.
[23] Huo, L., and Wang, Z. (2016), Service composition instantiation based on cross-modified artificial Bee Colony algorithm, China Communication, 13(10), 233-244.
[24] Patnaik, R., Padhy, N., and Raju, K.S. 2021, A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges. In Intelligent System Design, (pp. 723-730). Springer, Singapore.
[25] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congr. Serv., pp. 21–28, 2015.
[26] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014.
[27] Shafagh, H., Burkhalter, L., Hithnawi, A., and Duquennoy, S. (2017). "Towards blockchain-based auditable storage and sharing of IoT data," in Proceedings of the 2017 on Cloud Computing Security Workshop (New York), 45–50. doi: 10.1145/3140649.3140656
[28] Khan, A., and Salah, K., (2018), IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, Vol. (82), pp.395-411.
[29] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in the internet of things: Challenges, solutions, and future directions," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2016–March, pp. 5772–5781, 2016.
[30] Ng, I., and Wakenshaw, S., (2017), The IoT: Review and research directions, International Journal of Research in Marketing, Vol.34,No.1,pp.3-21.
[31] T. Wansinghe, R. Gosine, L. James, G. Mann, O. de Silva and P. Warian, (2020),The IoT in the Oil and Gas Industry: A Systematic Review, in IEEE IoT Journal, vol.7, No.9, doi: 10.1109/JIOT.2020.2995617.
[32] S. Birkel and E. Hartmann, (2019), Impact of IoT challenges and risks for SCM, Supply-Chain-Management, ISSN: 1359-8546
[33] Weber, H., (2010), Internet of Things – New security and privacy challenges. Computer Law and Security Review, Vol.26,pp.23-30.
[34] L., Da Xu, W. He, and S. Li, (2014),IoT in industries: A survey, IEEE Transactions on Industrial Informatics,Vol.10, No.4,pp.2233-2243.
[35] Laboratoire International de Recherche en Informatique et Mathématiques Appliquées, Available online: Available: https://lirima.inria.fr/fr/focus-on-a-joint-project-team-iot4d/ (accessed on 9 Sep 2022).
[36] Y. Yang, L. Wu, G. Yin, L. Li & H. Zhao, (2017), A Survey on Security and Privacy Issues in IoT, in IEEE Internet of Things Journal, Vol.4, No.5, pp.1250-1258.
[37] Sachin S., Angappa G., Harsh P., Sudhanshu J., Modeling the IoT adoption barriers in food retail supply chains, Journal of Retailing and Consumer Services, ISSN 0969-6989, doi.org/10.1016/j.jretconser.2019.02.020.
[38] M., Ahlmeyer, and M., Chircu, (2016),Securing the IoT:A review. Issues in Information Systems,Vol.17,No.4,pp.21-28.
[39] A., Karkouch, H., Mousannif, H., Al Moatassime, and T., Noel, (2016), Data Quality in IoT: A State of the Art Survey, JNCA, ISSN 1084-8045, doi.org/10.1016/j.jnca.2016.08.002.
[40] N., Côrte, P., Ruivo, & T., Oliveira, (2020), Leveraging IoT and Big Data Analytics Initiatives in European and American Firms, Information and Management, ISSN 0378-7206, doi.org/10.1016/j.im.2019.01.003.
[41] K. Kinder, "The Societal Impact of the Internet of Things," 2013.
[42] J. Ding, M. Nemati, C. Ranaweera and J. Choi, "IoT Connectivity Technologies and Applications: A Survey," in IEEE Access, vol. 8, pp. 67646-67673, 2020, doi: 10.1109/ACCESS.2020.2985932.
[43] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), 2016, pp. 1-4, doi: 10.1109/ICBDSC.2016.7460395.

[44] T., Lynn, P., Rosati, & T. Endo, (2018), Toward the Intelligent Internet of Everything: Observations on Multidisciplinary Challenges in Intelligent Systems Research, In: Picazo-Vela, S., Hernández L. R. (eds.) Technology, Science, and Culture: A Global Vision, vol. 116, pp. 52–64.
[45] M. N. S. Miazi, Z. Erasmus, M. A. Razzaque, M. Zennaro, and A. Bagula, ‘‘Enabling the Internet of things in developing countries: Opportunities and challenges,’’ in Proc. 5th Int. Conf. Informat., Electron. Vis. (ICIEV), Dhaka, Bangladesh, May 2016, pp. 564–569.
[46] Rey, A.; Panetti, E.; Maglio, R.; Ferretti, M. Determinants in adopting the Internet of Things in the transport and logistics industry. J. Bus. Res. 2021, 131, 584–590.
[47] P. Rosati, and T. Lynn, (2020), Mapping the Business Value of the Internet of Things. In: Lynn, T., Mooney, J., Lee, B., Endo, P. (eds) The Cloud-to-Thing Continuum. Palgrave Studies in Digital Business and Enabling Technologies. Palgrave Macmillan, Cham. doi.org/10.1007/978-3-030-41110-7_8
[48] P. Rosati, G. Fox, D. Kenny, and T. Lynn., (2017), Quantifying the Financial Value of Cloud Investments: A Systematic Literature Review. 2017 IEEE International Conference on Cloud Computing Technology and Science, pp.194–201.
[49] H.-D. Ma, “Internet of things: Objectives and scientific challenges,” Computer Science and Technology, Springer, vol. 26, no. 6, 2011
[50] J. P. Meltzer, (2019), “Global Views Globalviews Artificial intelligence primer:,” no. 12, 2019.
[51] Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., & Urien, P. (2015). Internet of Things: A Definition & Taxonomy. 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies. doi:10.1109/ngmast.2015.71
[52] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Netw., 10(7), 1497 (2012).
[53] A. H. Crespo, M. M. G. de los Salmones, I. R. del Bosque, ´ et al., “Influence of users perceived compatibility and their prior experience on b2c e-commerce acceptance,” in Electronic Business and Marketing. Springer, 2013, pp. 103–123.
[54] Rybakov, A. (2021), Applying IoT to transform business: top-10 cases, AgileVision, Available online: https://www.agilevision.io/blog/applying-iot-to-transform-business-top-10-cases (accessed on 28 Sep 2022).
[55] Maras, M.-H. (2015). Internet of Things: security and privacy implications. International Data Privacy Law, 5(2), 99–104. doi:10.1093/idpl/ipv004
[56] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), 3rd International Conference on Recent Trends in Network Security and Applications, Chennai, India, 2010, pp.420–429.
[57] Chanopas, A., Krairit, D. and Khang, D. B. (2006). “Managing information technology infrastructure: a new flexibility framework”. Management Research News, Vol. 29, No. 10, pp. 632-651.
[58] Lund S. and Manyika, J., (2016), ``How digital trade is transforming globalisation," The E15 Initiative, Int. Centre Trade Sustain. Develop. (ICTSD) World Econ. Forum, Geneva, Switzerland, Tech. Rep. [Online].Available:http://www.e15initiative.org/andhttp://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation/
[59] I. Ehie, and M. Chlton, (2020), Understanding the influence of IT/OT Convergence on the adoption of IoT in manufacturing organisations, Computers in Industry, Vol.115, ISSN 0166-3615.
[60] Lee, S. and Kim, K. J. (2007) “Factors affecting the implementation success of Internet-based information systems”. Computers in Human Behavior, Vol. 23, No. 4, pp. 1853-1880.
[61] Yan Yu, Jianhua Wang, & Guohui Zhou. (2010). The exploration in the education of professionals in applied Internet of Things Engineering. 2010 4th International Conference on Distance Learning and Education. doi:10.1109/icdle.2010.5606038
[62] Yu Zhongcheng. The Internet of Things, the Next War We Can't Afford to Lose [J].China Computer & Communication,20 10(3)44-46.
[63] Botha, R. A. and Eloff, J. H. P. (2001), “A framework for access control in workflow systems”, Information Management & Computer Security, 9/3, pp. 126-133.
[64] Blobel, B., Nordberg, R., Davis, J. M. and Pharow, P. (2006), “Modelling privilege management and access control”, International Journal of Medical Informatics, 75, pp. 597-623

© 2022 By AIRCC Publishing Corporation. This article is published under the Creative Commons Attribution (CC BY) license.