



# Technological Variables for Decision-making IoT Adoption in Small and Medium Enterprises

Diana Teresa Parra <sup>1\*</sup>, César D. Guerrero <sup>1</sup>

<sup>1</sup>PhD in Engineering, Universidad Autonoma de Bucaramanga, Bucaramanga, COLOMBIA

\*Corresponding Author: [dparra486@unab.edu.co](mailto:dparra486@unab.edu.co)

**Citation:** Parra, D. T. and Guerrero, C. D. (2020). Technological Variables for Decision-making IoT Adoption in Small and Medium Enterprises. *Journal of Information Systems Engineering and Management*, 5(4), em0124. <https://doi.org/10.29333/jisem/8484>

## ARTICLE INFO

Published: 29 Aug. 2020

## ABSTRACT

The Internet of Things (IoT) is a key technological trend for the digital transformation of organizations, boosting existing information and communication technologies or the deployment of new IoT solutions to improve their business models. Decision-making IoT adoption in small and medium enterprises is a complex task led by the Chief Information Officer (CIO). The deployment of IoT solutions is affected by permanent technological change in the ICT sector. That implies high investment costs by organizations due to the acquisition of technology, maintenance of technology, training of employees for the appropriate use of each technology, and expensive contracts with the Internet of Things providers for the execution of IoT projects. This paper presents four technological variables that affect decision-making IoT adoption in small and medium enterprises based on the Technology-Organization-Environment Model (TOE). The role of the CIO in supporting the digital transformation of SMEs and the complexity of IoT adoption are highlighted.

**Keywords:** decision-making, digital transformation, IoT adoption, small and medium enterprises, TOE framework

## INTRODUCTION

The Internet of Things (IoT) is a technological trend that implies the pervasive presence in the environment of a variety of objects connected to the Internet through multiple networks that can interact with each other to reach common goals (Atzori, Iera and Morabito, 2010). Internet of Things adoption represents a high level of complexity for organizations since not only a new software or hardware tool is adopted (Assante *et al.*, 2018; Carcary *et al.*, 2018). It is about deploying technological solutions based on conceptual frameworks or IoT architectures that present layers, technologies, protocols, and devices, establishing relationships between them, considering requirements such as connectivity, interoperability, and security and privacy (International Telecommunication Union, 2012b). This scenario implies that the Chief Information Officer (CIO) proposes a digital transformation strategy based on the Internet of Things technologies, taking into consideration the business model of the organization and the human, financial, and technological resources that the organization possesses. Additionally, as the company employees lack knowledge about the potential of the Internet of Things, the use of providers to support the IoT project from technology selection, architecture development, and project implementation is required to reduce project risk (Gartner, 2017b).

Organizations can initially propose small IoT projects and carry out proofs of concept before broad deployment to the entire organization (Gartner, 2019). An example of this process is the integration of e-Commerce with the Internet of Things as a strategy to improve the customer experience (Shen and Liu, 2010). Regarding technology readiness, the organization requires Internet connectivity through a plan contracted with an Internet Service Provider. Employees must have digital skills to use traditional information and communications technologies, such as e-mail, electronic transactions, customer service, and information searching. A desirable scenario for companies is to have employees with knowledge on the Internet of Things, who can support providers during all phases for the deployment of IoT projects. In this sense, the CIO must formulate policies on ownership, sharing, management, and usage of the data generated by the IoT solutions (Gartner, 2017b). In the case of small and medium enterprises, IoT adoption implies a higher risk than large companies due to its technological and economic limitations (Organisation for Economic Cooperation and Development, 2017).

We organize this paper as follows. Section "Theoretical Background" presents a theoretical background of IoT adoption in small and medium enterprises based on the synthesis of seven documents found in the literature. Section "IoT Adoption in Small and Medium Enterprises" offers the life cycle of an IoT project, the structure of the technological factor based on the TOE framework, and the definition of four adoption variables (Cost, ICT infrastructure, R&D activities, and Security and privacy). Finally, last section presents our conclusions.

## THEORETICAL BACKGROUND

In the literature, we found documents about IoT adoption published during 2016-2019 in the following academic databases: ACM Digital Library, Emerald Insight, IEEE Xplore Digital Library, Science Direct, and Springer Link. We used the following descriptors: Internet of Things, small and medium enterprises, and IoT adoption. The selected documents (belonging to two major disciplines: Information Systems and Information Technology, and Business, Management & Strategy) presented theoretical aspects about the Internet of Things, and the level of complexity for small and medium enterprises to adopt the Internet of Things solutions because IoT requires the adoption of hardware, software and networking technologies reflecting a wide variety of technologies, protocols, and devices (Patel and Cassou, 2015). We present the selected documents in chronological order below:

Lee and Lee (2015) presented five IoT technologies that are necessary to the deployment of IoT-based products and services: Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Middleware, Cloud Computing, and IoT application software. The authors discussed three IoT categories of real-world IoT applications that enhance customer value: Monitoring and control, Big Data and business analytics, and Information sharing and collaboration (Lee and Lee, 2015).

Abazi (2016) explained the process that must be followed by small and medium enterprises for decision-making IoT adoption, indicating that owners, managers, and employees must know about the Internet of Things and their impact on the organization. The author identified two aspects required for IoT adoption in SMEs: Infrastructure (related to Internet access, network technologies, network speed, and quality), and Regulation (policies that favor the digital transformation of organizations, for example, funding, financial support, subsidies) (Abazi, 2016).

Nylander et al. (2017) presented a case study about a company that developed a connected product without competencies in the Internet of Things. The authors carried out multidisciplinary research (collaboration between computer science, business model research, and product development research), indicating that the organization must initially acquire technical skills to deploy Internet of Things solutions. Besides, R&D activities in the IoT domain are necessary to address challenges related to standards, interoperability, and security (Nylander, Wallberg and Hansson, 2017).

Shin (2017) presented an exploratory study of Innovative Korean IoT-SMEs, analyzing the definition of the Internet of Things and policy implications. The author elaborated an extensive literature review related to IoT, SMEs innovation, and sustainable growth strategy, and conducted individual interviews in 40 companies during September 2014. As a result, the author suggests that small and medium enterprises have possibilities with the Internet of Things solutions to improve their business models (Shin, 2017).

Assante et al. (2018) described the early activity of the European project Internet of Things for European Small and Medium Enterprises (IoT4SMEs). The survey was distributed to IoT experts, managers, and professionals linked to 800 small and medium enterprises from countries of the IoT4SMEs partnership. The authors concluded that Internet of Things is a complex technological trend, with high impact in several economic sectors (e.g., Information and Communication Technologies, Services, Industry, Consulting, Retail, Telecommunication, Manufacturing, Healthcare, Transport/Logistics, Agriculture, Food, and Banking) (Assante et al., 2018).

Carcary et al. (2018) examined existing literature related to factors that influence IoT adoption in organizations. The authors studied the Unified Theory of Acceptance and Use of Technology constructs to identify the applicability of UTAUT in the Internet of Things domain, indicating that IoT is a complex and sophisticated technological trend. The following UTAUT constructs could explain the drivers, benefits, barriers, and challenges: Performance expectancy, Social influence, and Facilitating conditions (Carcary et al., 2018).

Lee (2019) presented an IoT ecosystem, IoT architecture, and the IoT service business model required to deploy IoT services in enterprises. The IoT ecosystem consists of five key players: software platform developers, hardware platform developers, network technology developers, application/solution developers, and users and customers. The IoT architecture presented consists of five layers: Perception layer, Network layer, Processing layer, Application layer, and Service management layer. The IoT service business model has four essential components: value proposition, networking activities, resources, and sustainability (Lee, 2019).

**Table 1** shows the selected documents on IoT adoption. We extracted the following data from each paper: (1) Concepts: IoT applications, IoT challenges, IoT ecosystem, IoT investment, IoT security, IoT strategy, IoT technologies, and (2) Paper classification: Concept paper, Research paper, and Review paper.

Small and medium enterprises are vital for a healthy economy since they are responsible for a significant contribution to valued-added and creation of new jobs. However, they have limitations related to the lack of technological and financial resources, and employees that don't have adequate digital skills prevent them from being competitive in the market (Organisation for Economic Cooperation and Development, 2017). The Internet of Things is a technological trend that is changing the way of doing business. IoT solutions can be an opportunity for small and medium enterprises to improve their business models through digital innovation (Lee, 2019). IoT adoption suggests an economic challenge for SMEs to achieve a high level of technological preparation. In this case, the organization must assume additional costs for the fulfillment of the following activities: deployment of sophisticated technological infrastructure that is compatible with Internet of Things technologies, training of employees for the proper use of Internet of Things solutions, hiring external IoT providers for the execution of IoT projects, financing research, and development activities for the deployment of IoT solutions, among others.

**Table 1.** The IoT adoption concept matrix and paper classification

Citation	Concepts							Paper classification		
	IoT applications	IoT challenges	IoT ecosystem	IoT investment	IoT security	IoT strategy	IoT technologies	Concept paper	Research paper	Review paper
(Lee and Lee, 2015)	X			X	X		X	X		
(Abazi, 2016)		X			X			X		
(Nylander, Wallberg and Hansson, 2017)		X	X							X
(Shin, 2017)			X							X
(Assante et al., 2018)							X			X
(Carcary et al., 2018)		X		X	X	X				X
(Lee, 2019)	X		X							X

**Table 2.** Technological variables that describes IoT adoption in SMEs

Variable	Definition
Cost	"Total cost of using information and communications technologies" (Ghobakhloo, Arias-Aranda and Benitez-Amado, 2011).
ICT infrastructure	"Access to network services to support web and Internet technologies" (Awa and Ojiabo, 2016).
R&D activities	"Measures the percentage of firm's technologies / products / systems that result from internal R&D or R&D collaborations" (Giotopoulos et al., 2017).
Security and privacy	"Privacy and confidentiality of the companies' data" (Tehrani and Shirazi, 2014).

## IoT ADOPTION IN SMALL AND MEDIUM ENTERPRISES

The Internet of Things will impact the economy through the digital transformation of small and medium enterprises, facilitating new business models (Gartner, 2017a) and boosting their productivity and competitiveness (Alshamaila, Papagiannidis and Li, 2013; Consoli, 2012; Qureshi, 2005), thus impacting economic and social development prospects (International Telecommunication Union, 2017b). One of the main barriers that affect IoT adoption in companies is the complexity and the lack of knowledge about the use of technology. In the case of small and medium enterprises added to the barriers mentioned above, the adoption of IoT solutions is more complex, considering its technological and economic limitations. Companies must understand how IoT adoption can promote their digital transformation. IoT adoption implies for companies the design of projects preceded by the CIO. The Internet of Things projects has long execution times, high investment, and multidisciplinary project teams working for a common purpose. According to Gartner, the life cycle of an IoT project has three main phases (Gartner, 2017b):

**First phase: Objective and strategy setting.** In this phase, the team project identifies the process, product, or service that will be modified to obtain better results in the organizations. These include resources optimization, business strategy, business opportunities, improvement of processes, competitive differentiation, customer satisfaction, increasing profits, among others.

**Second phase: Technology selection, architecture development, and project implementation.** The team project carries out research and development activities to identify existing IoT solutions in the telecommunications market aligned with the business model and the deployment and management of the IoT solutions.

**Third phase: Ongoing operations.** Phase related to the organization's activities to guarantee the availability, performance, and security and privacy of the technological solution, which implies permanent supervision and maintenance activities.

For small and medium enterprises to properly face a digital transformation based on the Internet of Things, employees need to receive training for the proper use of IoT solutions. Employees must have digital skills, which have allowed them to perform in the organization so far, for example, using traditional IT devices to send and receive an e-mail, consumer service, accessing e-commerce, and e-banking services. The CIO of the company should lead the training strategy. Besides, companies should have staff with IT training, if possible, to have an Information Technology department. Small and medium enterprises should have an Internet connection in their facilities and a website. The use of information and communication technologies varies depending on the economic sector to which small and medium enterprises belongs (e.g., the manufacturing industry sector, trade sector, or services sector).

The technological factor that describes IoT adoption in small and medium enterprises was defined, taking into consideration the Technology-Organization-Environment Model (TOE) (Tornatzky, Fleischer and Chakrabarti, 1990). TOE framework is a theory at the organizational level, which explains how a company's context influences the adoption and implementation of technological innovations (Baker, 2012). According to Tornatzky et al. (1990), the technological factor refers to aspects related to information and communication technologies that the organization has acquired (e.g., hardware, software, and networks technologies) and those that are available in the telecommunications market according to technological trends (Tornatzky, Fleischer and Chakrabarti, 1990). Based on the literature review, we defined four variables that belong to the technological factor (Parra and Guerrero, 2020): Cost, ICT infrastructure, R&D activities, and Security and privacy (see Table 2). Next, we present the definitions and aspects related to each one of the identified technological variables.

### Cost

The cost of IoT deployment differs mainly from the adoption of traditional information and communication technologies (e.g., Internet, e-mail, website, e-Commerce) in terms of their complexity. Therefore, the CIO must contemplate technological,

organizational, and environmental aspects to reduce project risk, and calculate an estimated cost of investment, taking into consideration two scenarios:

1. The IoT project will be integrated with existing information and communication technologies to enhance them, such as boost e-Commerce (Yu and Zhang, 2017) or favor the deployment of multiple solutions in the organization incorporating technological trends like Cloud Computing (Botta *et al.*, 2016).
2. The IoT project is a new technological solution based on the Internet of Things that requires technological readiness to promote the digital transformation for the improvement of processes, products, or services. In both cases, the CIO will be leading a proof of concept or even pilot tests to justify IoT investments from successful results in early stages of IoT adoption, since the cost to deploy IoT solutions is usually higher than expected.

Among the costs that must be assumed by small and medium enterprises for the execution of IoT projects, the following stand out: hire staff with knowledge on Internet of Things from different areas (e.g., Computer Science, Engineering, Decision Sciences, Social Sciences, Energy, Business, Management and Accounting), with skills to participate in technological innovation processes; train employees for the acquisition of new digital skills to follow the digital transformation for the appropriate use of key IoT technologies (e.g., training courses related to basic competences about IoT, new business models, IoT technologies and applications, legal aspects related to IoT, IT hardware support, data analysis, networking and security); develop substantial changes in the technological infrastructure for the deployment of IoT solutions that responds to the needs of the organization, that will accelerate the transformation process of the company; and hire external Internet of Things providers for technology selection, architecture development and project implementation.

### ICT Infrastructure

The deployment of technological solutions of the Internet of Things in small and medium enterprises involves transforming the existing ICT infrastructure in the organization to support IoT trends and technologies (Gartner, 2018b). Information and communication technologies infrastructure encompass fixed-telephone, mobile-cellular, fixed-broadband, and other technologies (International Telecommunication Union, 2018). The execution of IoT projects requires broadband infrastructure, which presents limitations in developing countries due to the lack of connectivity to ICT backbones. Its development requires improved policies in developing economies as a strategy to favor economic development and the growth of the IoT ecosystem. The IoT project team can follow the guidelines established by the International Telecommunications Union for the deployment of IoT solutions in organizations.

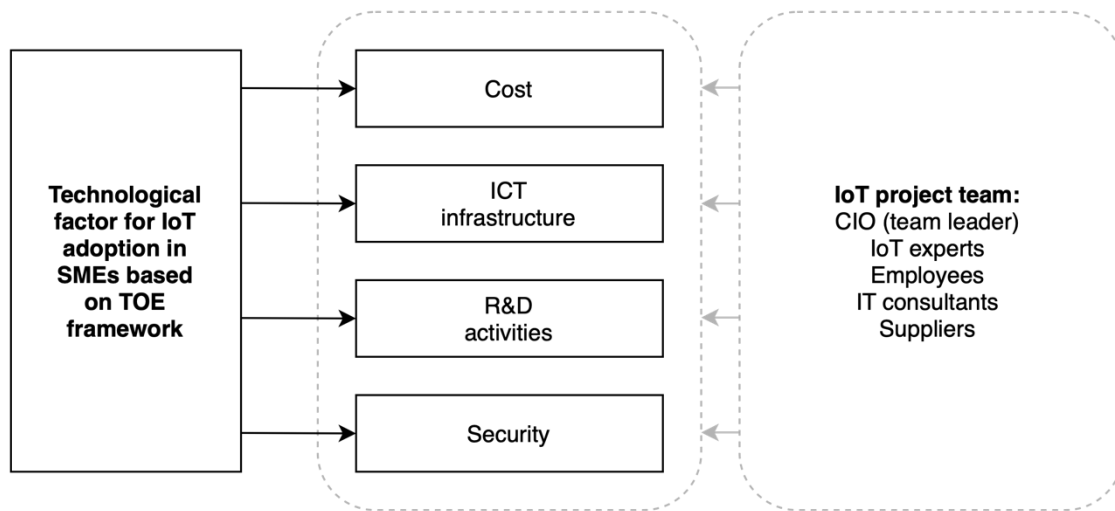
According to Recommendation ITU-T 4113: Requirements of the network for the Internet of Things, the reference network model for IoT solutions comprises three parts: core network, access network, and IoT area network (International Telecommunication Union, 2016). The core network connects the service provider domain with the access network acquired by the company through a contract with an Internet Service Provider, which has coverage in the location of the company. The access network connects the IoT devices using different technologies, such as Public Switched Telephone Network (PSTN) technology, 2G/3G/LTE wireless technology, Digital Subscriber Line (DSL) technologies, Fiber to the x (FTTx) technology, and Low-Power Wide-Area (LPWA) wireless technology. This infrastructure needs constant investment to improve the network's quality and capacity (International Telecommunication Union, 2018). Finally, the IoT area network conformed by IoT devices and gateways uses one or more of the following technologies: Radio Frequency Identification (RFID), ZigBee wireless technology based on IEEE 802.15.4, Bluetooth wireless technology based on IEEE 802.15.1, and Wi-Fi wireless technology known as IEEE 802.11.

### R&D Activities

Considering the complexity that suggests the deployment of Internet of Things solutions, small and medium enterprises must have a CIO that identifies the benefits that the organization can obtain from the IoT adoption. In this case, the CIO will be leading the technological innovation process to improve/create processes, products, or services. The main functions of the CIO would be:

1. Formulate policies for IoT adoption in the organization that favors the digital transformation.
2. Propose strategies for the execution of IoT projects, contemplating technological, organizational, and environmental aspects to reduce project risk.
3. Define the training courses for employees related to the appropriate use of IoT solutions and the acquisition of new competencies and digital skills to face technological change.
4. Establish alliances with the IoT ecosystem's strategic actors for the successful deployment of Internet of Things solutions (e.g., Internet Service Providers, IT consultants, Suppliers, Universities, Financial entities, Governmental agencies, Standards organizations).

The execution of IoT projects requires professionals from different areas of knowledge and the support of suppliers to participate in research and development activities, including basic research, applied research, and experimental development. The IoT project team can define its strategy based on standards issued by specialized agencies for information and communication technologies, such as the International Telecommunication Union (ITU). For the implementation of IoT solutions, ITU Telecommunication Standardization Sector (ITU-T) has the Recommendations Y series that corresponds to "Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities," and specifically the Y.4000-Y.4999 series that deals with "Internet of things and smart cities and communities," among there are: Recommendation ITU-T Y.4000/Y.2060: Overview of the Internet of Things (International Telecommunication Union, 2012b), Recommendation ITU-T Y.4050/Y.2069: Terms and definitions for the Internet of Things (International Telecommunication Union, 2012a), and



**Figure 1.** Technological factor for IoT adoption in SMEs based on TOE framework

Recommendation ITU-T Y.4113: Requirements of the network for the Internet of Things (International Telecommunication Union, 2016).

### Security and Privacy

The development of the IoT solutions in organizations involves addressing security threats towards confidentiality, authenticity, and integrity of data and services (Chellappan and Sivalingam, 2016). One of the main consequences of vulnerabilities is the damage to organizations' reputation (e.g., affecting customer privacy), which in some cases involves costly lawsuits (Ziegeldorf, Morchon and Wehrle, 2014). According to Gartner, companies worldwide to protect themselves from IoT-based attacks will spend on IoT security \$3.1 billion in 2021 (Gartner, 2018a). Small and medium enterprises should consider investing in IoT security despite their financial limitations, taking into consideration the IoT reference model presented in Recommendation ITU-T Y.4000/Y.2060, which incorporates security capabilities, classified in two categories (International Telecommunication Union, 2012b): generic security capabilities (independent or included in the application, network, and device layer, e.g., authorization, authentication, access control, data confidentiality, device integrity validation) and specific security capabilities (linked to the application-specific requirements, e.g., mobile payment). Besides, the IoT project team can use the following documents, to provide security and privacy to the actors involved with the IoT solution: (1) Recommendation ITU-T X.1205: Overview of cybersecurity; presents a taxonomy of the security threats that can affect the organization (International Telecommunication Union, 2008), and (2) ITU-T Y.4806: Security capabilities supporting safety of the Internet of Things; presents security threats that may affect safety and security capabilities of Internet of Things (International Telecommunication Union, 2017a).

According to Lee and Lee (2015), lack of security and privacy affects the IoT adoption in companies (Lee and Lee, 2015). One way to deal with this problem is related to the training of IoT professionals to deploy secure solutions based on R&D activities. In this sense, the CIO could collaborate with the chief information security officer (CISO), to ensure that qualified staff with IoT security skills is involved in the IoT project team. Also, The CIO could participate in the acquisition of IoT devices and software tools to deploy secure IoT systems (Gartner, 2018b). In the case of small and medium enterprises, they must guarantee the development of IoT solutions with strong security to face cyber-attacks. The threats that affect the Internet of Things solutions are classified into three broad categories (Chellappan and Sivalingam, 2016): Capture (is responsible for capturing information), Disrupt (corresponds to denying, destroying, and disrupting the IoT solution); and Manipulate (related to data manipulation). Attacks on the Internet of Things infrastructure can be passive threats (eavesdropping or monitoring of transmissions) or active threats (masquerading, Man-in-the-middle, Replay attacks, Denial-of-Service (DoS) attacks).

**Figure 1** presents the technological factor consisting of four variables and the IoT project team conformed by the CIO, IoT experts, employees, IT consultants, and suppliers.

The decision-making process for IoT adoption is a complex task affected by the permanent technological change in the information and communications technologies sector. If organizations have invested before in other forms of ICT, they have a higher orientation towards new technologies. But if they had bad experiences in the past, the adoption process has a higher level of complexity, reinforced by resistance to technological change. Although the CEO is the one who finally makes the decisions in the organization according to his management style (autocratic, democratic, and liberal) (Čudanov, Todorović and Jaško, 2012), the CIO is the leader of the process for IoT adoption to improve/create processes, products or services. Besides, the CIO is responsible for ensuring the technological preparation, forming the IoT project team for the deployment of IoT solutions in the organization, and interacting with the key actors of the IoT ecosystem (Gartner, 2017b).

The technological preparation of the organization depends on the investment allocated to guarantee ICT infrastructure that supports the deployment of IoT technologies, as well as the training of the employees of the organization for the appropriate use of Internet of Things solutions. IoT brings value to enterprises when IoT devices communicate with each other and integrated with existing ICT solutions in the organization (e.g., customer support systems, business intelligence applications, business analytics,

and e-Commerce) (Lee and Lee, 2015). Companies will invest in the deployment of IoT solutions to generate innovations in organizational processes, favor the customer service process, improve tracking of products, optimize distribution costs, and increase revenues through significantly enhanced services to consolidate as market leaders. To be competitive in the market, small and medium enterprises should understand the importance of investing in information and communications technologies and R&D activities to deploy secure IoT solutions.

## CONCLUSION

The deployment of IoT business solutions will guide the digital transformation in small and medium enterprises. This process will be led by the CIO, who must face the complexity of IoT adoption considering three factors: technological, organizational, and environmental). Besides, the CIO will define the strategies to reduce project risk, considering the limitations that prevent the growth of SMEs (e.g., lack of financial capacity, lack of ICT infrastructure, and lack of IoT knowledge). The IoT project team will consist of professionals from different disciplines, working to optimize processes, products, and services of the organization. Decision-making IoT adoption in SMEs depends on the CEO considering his innovativeness, knowledge about the Internet of Things, and previous experiences with information and communication technologies (e.g., e-Commerce, e-Business, and Cloud Computing). From the technological point of view, although the cost of the IoT solution constrains IoT adoption decision-makers, existing ICT infrastructure, R&D activities, and Security and privacy, are variables to consider in the adoption of IoT solutions in SMEs.

## REFERENCES

- Abazi, B. (2016). An approach to the impact of transformation from the traditional use of ICT to the Internet of Things: How smart solutions can transform SMEs. *IFAC-PapersOnLine*, 49(29), 148-151. <https://doi.org/10.1016/j.ifacol.2016.11.091>
- Alshamaila, Y., Papagiannidis, S. and Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management*, 26(3), 250-275. <https://doi.org/10.1108/17410391311325225>
- Assante, D., et al. (2018). Internet of Things education: Labor market training needs and national policies. In *2018 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, pp. 1846-1853. <https://doi.org/10.1109/EDUCON.2018.8363459>
- Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
- Awa, H. O. and Ojiabo, O. U. (2016). A model of adoption determinants of ERP within T-O-E framework. *Information Technology & People*, 29(4), 901-930. <https://doi.org/10.1108/ITP-03-2015-0068>
- Baker, J. (2012). The Technology-Organization-Environment Framework. In Dwivedi, Y. K., Wade, M. R., and Schneberger, S. L. (eds.) *Information Systems Theory. Explaining and Predicting Our Digital Society, Vol. 1*. Springer, New York, NY, pp. 231-245. [https://doi.org/10.1007/978-1-4419-6108-2\\_12](https://doi.org/10.1007/978-1-4419-6108-2_12)
- Botta, A., et al. (2016). Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, 56, 684-700. <https://doi.org/10.1016/j.future.2015.09.021>
- Carcary, M., et al. (2018). Exploring the Determinants of IoT Adoption: Findings from a Systematic Literature Review. In *Perspectives in Business Informatics Research*, pp. 113-125. [https://doi.org/10.1007/978-3-319-99951-7\\_8](https://doi.org/10.1007/978-3-319-99951-7_8)
- Consoli, D. (2012). Literature Analysis on Determinant Factors and the Impact of ICT in SMEs. *Procedia - Social and Behavioral Sciences*, 62, 93-97. <https://doi.org/10.1016/j.sbspro.2012.09.016>
- Čudanov, M., Todorović, I. and Jaško, O. (2012). Correlation between soft organizational features and development of ICT infrastructure. In *Proceedings of the Fifth Balkan Conference in Informatics on - BCI '12*. New York, New York, USA: ACM Press, pp. 150-155. <https://doi.org/10.1145/2371316.2371345>
- Chellappan, V. and Sivalingam, K. M. (2016). Security and privacy in the Internet of Things. In *Internet of Things*. Elsevier, pp. 183-200. <https://doi.org/10.1016/B978-0-12-805395-9.00010-1>
- Gartner (2017a). *Leading the IoT, Gartner Insights on How to Lead in a Connected World, Gartner Research*. USA. Available at: [https://www.gartner.com/imagesrv/books/iot/iotEbook\\_digital.pdf](https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf)
- Gartner (2017b). *Three Strategies to Achieve Better-Than- Planned Outcomes for IoT Projects*. USA. Available at: <https://www.gartner.com/doc/3820163>
- Gartner (2018a). *Forecast: IoT Security, Worldwide, 2018*. USA. Available at: <https://www.gartner.com/doc/3863770>
- Gartner (2018b). *Top Strategic IoT Trends and Technologies Through 2023*. USA. Available at: <https://www.gartner.com/doc/3890506>
- Gartner (2019). *Hype Cycle for the Internet of Things, 2019*. USA. Available at: <https://www.gartner.com/doc/3947474>
- Ghobakhloo, M., Arias-Aranda, D. and Benitez-Amado, J. (2011). Adoption of e-commerce applications in SMEs. *Industrial Management & Data Systems*, 111(8), 1238-1269. <https://doi.org/10.1108/02635571111170785>
- Giotopoulos, I., et al. (2017). What drives ICT adoption by SMEs? Evidence from a large-scale survey in Greece. *Journal of Business Research*, 81(December 2016), 60-69. <https://doi.org/10.1016/j.jbusres.2017.08.007>

- International Telecommunication Union (2008). *ITU-T X.1205 (04/2008) Overview of cybersecurity*. Geneva, Switzerland. Available at: <https://www.itu.int/rec/T-REC-X.1205-200804-I>
- International Telecommunication Union (2012a). *ITU-T Y.4050 / Y.2069 (07/2012) Terms and definitions for the Internet of Things*. Geneva, Switzerland. Available at: <https://www.itu.int/rec/T-REC-Y.4050/en>
- International Telecommunication Union (2012b). *UIT-T Y.4000 / Y.2060 (06/2012) Overview of the Internet of Things*. Geneva, Switzerland. Available at: <https://www.itu.int/rec/T-REC-Y.4000/en>
- International Telecommunication Union (2016). *ITU-T Y.4113 (09/2016) Requirements of the network for the Internet of Things*. Geneva, Switzerland. Available at: <https://www.itu.int/rec/T-REC-Y.4113/en>
- International Telecommunication Union (2017a). *ITU-T Y.4806 (11/2017) Security capabilities supporting safety of the Internet of things*. Geneva, Switzerland. Available at: <https://www.itu.int/rec/T-REC-Y.4806-201711-I>
- International Telecommunication Union (2017b). *Measuring the Information Society Report 2017*. Geneva, Switzerland. Available at: <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017.aspx>
- International Telecommunication Union (2018). *Measuring the Information Society Report 2018*. Geneva, Switzerland. Available at: <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx>
- Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things*, 7, 100078. <https://doi.org/10.1016/j.iot.2019.100078>
- Lee, I. and Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431-440. <https://doi.org/10.1016/j.bushor.2015.03.008>
- Nylander, S., Wallberg, A. and Hansson, P. (2017). Challenges for SMEs entering the IoT world: success is about so much more than technology. In *Proceedings of the Seventh International Conference on the Internet of Things - IoT '17*. New York, New York, USA: ACM Press, pp. 1-7. <https://doi.org/10.1145/3131542.3131547>
- Organisation for Economic Cooperation and Development (2017). *Aid for Trade at a Glance 2017. Promoting Trade, Inclusiveness and Connectivity for Sustainable Development*. Paris: OECD Publishing. [https://doi.org/10.1787/aid\\_glance-2017-en](https://doi.org/10.1787/aid_glance-2017-en)
- Parra, D. T. and Guerrero, C. D. (2020). Decision-making IoT adoption in SMEs from a technological perspective. In *15th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE Xplore, pp. 1-6. <https://doi.org/10.23919/CISTI49556.2020.9141045>
- Patel, P. and Cassou, D. (2015). Enabling high-level application development for the Internet of Things. *Journal of Systems and Software*, 103, 62-84. <https://doi.org/10.1016/j.jss.2015.01.027>
- Qureshi, S. (2005). How does information technology effect development? Integrating theory and practice into a process model. In *AMCIS 2005 Proceedings*. Omaha, NE, USA, pp. 500-509.
- Shen, G. and Liu, B. (2010). Research on Application of Internet of Things in Electronic Commerce. In *2010 Third International Symposium on Electronic Commerce and Security*. IEEE, pp. 13-16. <https://doi.org/10.1109/ISECS.2010.11>
- Shin, D.-I. (2017). An exploratory study of innovation strategies of the internet of things SMEs in South Korea. *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(2), 171-189. <https://doi.org/10.1108/APJIE-08-2017-025>
- Tehrani, S. R. and Shirazi, F. (2014). Factors influencing the adoption of cloud computing by Small and Medium size Enterprises (SMEs). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8522 LNCS(Part 2), 631-642. [https://doi.org/10.1007/978-3-319-07863-2\\_60](https://doi.org/10.1007/978-3-319-07863-2_60)
- Tornatzky, L. G., Fleischer, M. and Chakrabarti, A. K. (1990). *Processes of technological innovation*. Lexington books.
- Yu, H. and Zhang, X. (2017). Research on the Application of IoT in E-Commerce. In *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*. IEEE, pp. 434-436. <https://doi.org/10.1109/CSE-EUC.2017.269>
- Ziegeldorf, J. H., Morchon, O. G. and Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, 7(12), 2728-2742. <https://doi.org/10.1002/sec.795>