IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 6, Ser. I (Nov - Dec 2019), PP 19-24
www.iosrjournals.org

Factors affecting IoT adoption

OMOYIOLA BAYO OLUSHOLA

School of Information Systems & Technology, Walden University, USA

Abstract: *Several organizations are behind in the implementation of the Internet of things (IoT) due to several factors. Some of these determinants are technological factors, organizational factors, and environmental factors. These factors include technology readiness, executive management support, compatibility, firm size, complexity, security concerns, regulatory support and intention to adopt Internet of Things.This paper explores some of the factors affecting IoT adoption, analyzing the determinants, other challenges, gaps, and future IoT developments.*

Keywords*: IoT, Framework, Constructs, Factors, Determinants, Adoption, and Influence*

Date of Submission: 16-11-2019 Date of Acceptance: 30-11-2019

I. Introduction

In this present age, competitive market condition, survival, and making profit in the market depend on factors such as competitive advantage, business agility, gains, flexibility, lower cost, and innovation. IoT can build worth and efficiencies across various sectorsthrough a vast system of smart things (Hsu & Lin, 2016; Voas, 2016). Since the Internet of Things is a recently developed technology, some technological factors, organizational factors, and environmental factors and other factors could impact the probability of its adoption. Research scholars portrayed numerous explanations behind the postponement of the adoption of Internet of Things, citing reasons, for example, lack of knowledge of the features of Internet of Thingsand its usefulness in different business areas (Hwang, Kim, & Rho, 2016; Hsu & Lin, 2016). It is essential to know the connection between these factors, and how organizations think before deciding to adopt Internet of Things. The reason for the research is to find the factors that impact the adoption of IoT in firms. In this paper, I present the background of problem, determinants affecting IoT, other factors affecting IoT, and future IoTopportunities.

1.1. Background of the problem

Firms usually look forward to having innovative and cutting-edge technologies that support efficiencies and business efficiency while reducing costsso they can survive for an extended period. Firms that neglect creativity are less nimble, adaptable, and competitive,and they don't last for long (Rosas, Brito, Palma, &Barata, 2017; Taneja, Pryor, & Hayek, 2016). Internet of Things is an innovative technology that can build a firm's worthwhile improving operational profitability (Hsu & Lin, 2016; Voas, 2016). A significant part of the development of the Internet of Things is relied upon to happen in the assembling division (Farooq, Waseem, Khairi, &Mazhar, 2015). Only a minority of firms have Internet of Things initiatives, and only a lesser percent of them have effectively incorporated Internet of Things frameworks (Ives, Palese, & Rodriguez, 2016). Internet of Things is a critical empowering agent to enhance development within the assembling division. Be that as it may, makers have been hesitant to embrace Internet of Things because of an absence of comprehension about the construct identified with Internet of Things reception and how their organization can apply Internet of Things effectively (Hwang et al., 2016; Oliveira, Thomas, &Espadanal, 2014). Scarcely any scientists have tended to Internet of Things adoption at the organization level (Hsu, and Lin, 2016b; Hwang et al., 2016; Singh, Gaur, & Ramakrishnan, 2017; Tu, 2018; Yang, Lee, & Zo, 2017a). Indeed, even fewer analysts have used a blend of diffusion of innovation (DOI) and technology-organization-environment framework (TOE) to research within the assembling area (Alkhalil, Sahandi, & John, 2017; Shaltoni, 2017; Wang & Wang, 2016). Through the literature audit, the elements influencing IoT adoptions was discovered. My objective for this research is to review past research and analyze the factors affecting IoT adoption in organizations.

II. Determinants affecting IoT adoption

The determinants affecting IoT are the intention to adopt and ten independent factors, which are technology readiness, compatibility, complexity, executive management support, firm size, regulatory support, security concerns, cost savings, compatibility and relative advantage. These factors can be seen in the integrated model in Figure 1 that combines theDOI Theory and TOE framework, a good model proposed by Oliveira et al.

(2014) which is a good framework for the study of IoT. This paper would be analyzing seven factors out of the ten independent factors and the dependent construct. The seven factors are technology readiness, compatibility, complexity, executive management support, firm size, regulatory support, and security concerns, and the dependent factor is the intention to adopt. Regulatory support, one of the seven independent constructs is an environmental context. Firm size and executive management support are organizational contexts. Technology readiness is technology context. Complexity and Compatibility, two constructs are innovation contexts and then we have security concerns. Some attributes were taken from DOI theory while some were taken from the TOE framework. The mixture covers the limitations of using only one. It is beneficial for identifying internal and external determinants and having a better understanding of innovation adoption (Alkhalil et al., 2017; Awa, Ojiabo, &Orokor, 2017; Cheng, 2015; Ji & Liang, 2016; Wang & Wang, 2016).

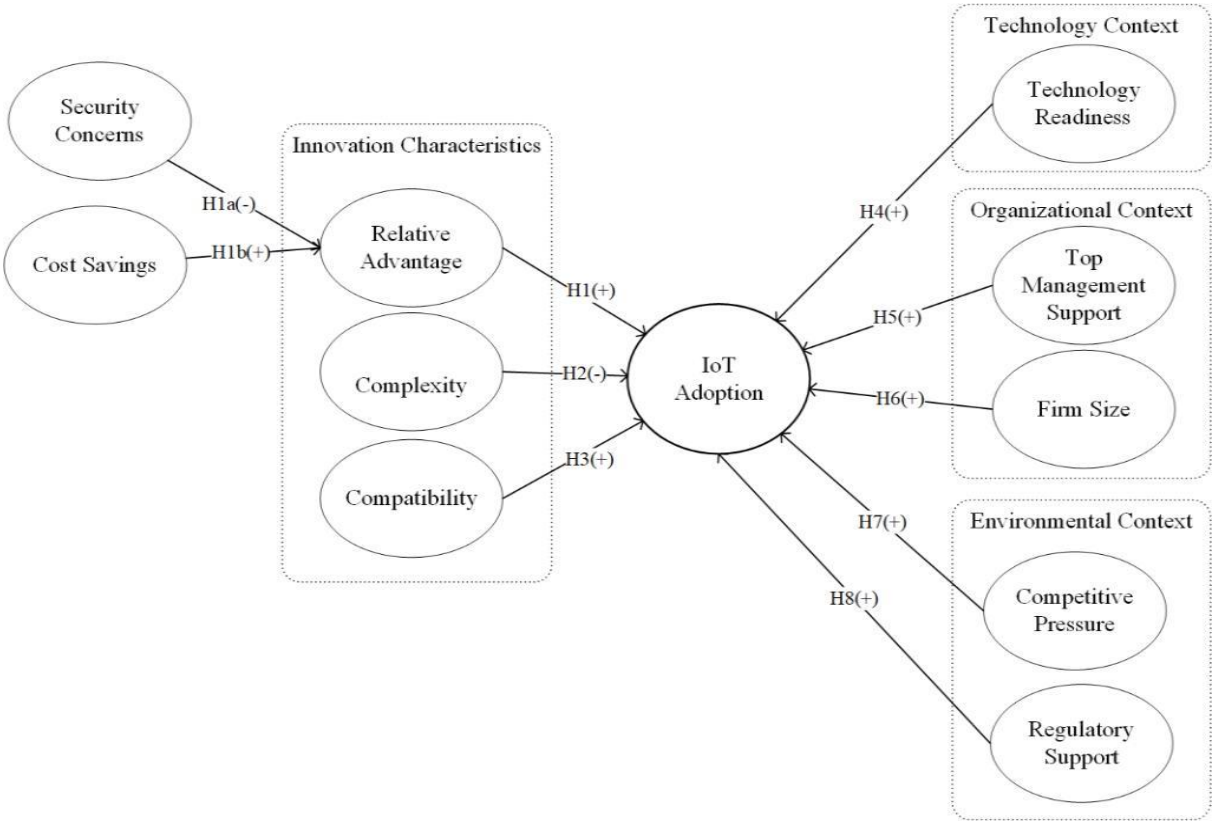

Figure 1. Integrative DOI-TOE model showing factors affecting IoT adoption (Oliveira, Thomas, &Espadanal, 2014).

2.1 Organizational context

The organizational context is explained by the executive management support and firm size constructs which are organizational-based factors.

2.1.1Executive management support: The executive management support holds a critical function in IoT adoption since it leads the unification of services, sharing of resources and the processes re-engineering (Hsu &Yeh, 2016; Martins et al., 2016; Wang & Wang, 2016). Without the influence and help of executive management, the company is likely to resist IoTadoption (Wang & Wang, 2016). Executive management support will positively affectIoT adoption.

2.1.2.Firm size: Big companies have more merits than small ones since they have more resources and can take more significant threats linked with innovation adoption (Carcary, Doherty, Conway, & McLaughlin, 2014). Small firms, although more adaptable, do not have the resources or knowledge to readily adopt newer technologies (Carcary et al., 2014). The size of a firm is a determinant of IoT adoption. The firm size will positively influence IoT adoption.

2.2. Environmental context

The environmental context is explained by the regulatory support factor which is environmental in nature as it is industry and governmentbased.

2.2.1. Regulatory support: The regulations of the government of nations can affect the adoption of IoT by firms. But IoT regulation is still evolving (Ahlmeyer&Chircu, 2016; Atzori, Iera, &Morabito; Hosek et al., 2017). If and whenever a government enforces IoT policy compliance with a huge amount of money to be paid by firms who do not comply, several companies would want to adoptIoT(Krotov, 2017; Ng & Wakenshaw, 2017). This Regulatory support will significantly affect IoT adoption.

2.3. Technology context

The technology context explains the technology readiness factor as it is a technology-related determinant.

2.3.1 Technology readiness: The technology context has to do with the organization, knowledge, and skills of the employees. The ability of technological infrastructures to easily integrate with IoT is a part of the organization structure (Rosas et al., 2017). A firm whose company with technological infrastructure and employees with updated IT knowledge and skills has a higher degree of technological readiness and thus is more likely to adopt IoT. These kinds of firms are in a good position to adopt IoT (Martins et al., 2016). Technology readiness positively impacts IoT adoption

2.4. Innovation characteristics

The innovation characteristics is explained by complexity, compatibility and security concerns which are innovation and design related.

2.4.1.Complexity: Complexity explains the level of difficulty in understanding and utilizinginnovation (Rogers, 2003). Complexity in IoT adoption is the difficulty level of the perception of IoT adoption and integration. Planning on and Selection from a wide range of IoT gadgets adds a level of complexity (Zhong, Xu & Wang, 2017). Complexities are not suitable for IoT adoption. Especially when there is no skilled employee in many the complex environment (Haddud, DeSouza, Khare, & Lee, 2017; Wang & Wang, 2016). Complexity will affect IoT adoption negatively

2.4.2. Compatibility: Compatibility explains the level that innovationunifies with present practices or value systems (Rogers, 2003). The rate of adopting a change is proportional to the compatibility level; therefore, the higher the compatibility, the quicker the adoption. Compatibility among technology systems is an important determinant that affects IoT adoption (Haddud et al., 2017; Ng & Wakenshaw, 2017). The compatibility will affect IoT adoption positively.

2.4.3. Security concerns: There are security risks and matters affecting IoT adoption. There are issues like security gaps, privacy and security concerns that affects the adoption of IoT(Ahlmeyer&Chircu, 2016; Balte, Kashid&Patil, 2015; Kumar, Vealey, & Srivastava, 2016; Sathish Kumar & Patel, 2014; Weber, 2015; Weinberg, Milne, Andonova, &Hajjat, 2015;Yuchen, Longfei, Guisheng, Lijie, &Hongbin, 2017).

2.5. The Intention for IoT adoption

The intent for IoT adoption is a primary factor in the study of IoT. The IoT has been evolving to grow. There are a lot of benefits to be gained from the evolution of IoT devices by making good use of the data from these devices (Atzori et al., 2017; Bi, 2017; Zhong et al., 2017); But the influence on the organizational business strategy, infrastructure, and security architecture must first be taken into consideration by organizations (Ahlmeyer&Chircu, 2016; Kumar et al., 2016). The intention to adopt IoT has not been fast even though most of the independent constructs has positive impact on IoT (Ives et al., 2016). There is need to address and consider factors such as cost and security concerns to enhance IoT adoption.

III. Other factors affecting IoT adoption

Borgia (2014) opined that the main challenges of the IoT vision are: data processing, architecture, communication, discovery, addressing, data management, privacy, and security, etc. The researcher explained that the solutions that cover all the challenges are not yet in existence. He suggested that standardization could enable IoT to prevent fragmentation while the interoperability of the solutions proposed is enabled (Borgia, 2014).Balte et al. (2015**)** opined thatthe challenges of IoT include: Scalability; Device heterogeneity; Energy-optimized solutions; Ubiquitous data exchange through wireless technologies; Localization and tracking capabilities; Embedded Security and privacy-preserving mechanisms, and Self-organization capabilities; Semantic interoperability and data management. Weinberg et al. (2015) opined that management challenge with privacy is now higher than ever before, because of the increase in the number of consumer-related data and access and tradeoffs in benefits linked with Internet of Things and human-related issues related to user experience. Yuchen et al. (2017) explained that there are privacy and security challenges with IoT and there are

limitations of IoTdevices in battery and computing resources and solutions. Da Xu et al. (2014) identified IoT challenges as standardization, cost of implementation, complication and privacy, and security.

Ahlmeyer&Chircu (2016) identified three IoT related gaps: Insufficient security in current IoT implementations, insufficient detailed and specific IoT guidelines in current IT security standards, and insufficient IoT laws and regulation at the country and international level. The researchers indicated that the IoT security issues include data breaches, identity theft, and hackings. The duo proposed an IoT security framework to address the gaps. The framework shows requirements in the areas of IoT security activities, scales, standards, value chains, and education(Ahlmeyer&Chircu, 2016).Atzori et al. (2017) indicated thatRFID platforms have missing IoT features such as autonomy and autonomic; practical object virtualization; interaction between objects; Pervasive computing platforms have missing IoT features such as Global network infrastructure; interfaces for thing to thing interactions; Cyber-physical systems have missing IoT features such as Global network infrastructure; Sensor networks have missing IoT features such as Global network infrastructure, pervasiveness, and heterogeneity of the technologies; M2M systems have missing IoT features such as Pervasiveness; autonomy and autonomicity. Hsu & Lin (2016) stated that their IoT study was limited to quantitative research. The statistical analysis was limited to numerical relationships, and the interpretation of the results was limited to the subjective appraisal of the author. The study was also limited to an online questionnaire served to self-selected respondents (Hsu & Lin, 2016). Weber (2015) identified a gap and suggested that there is a need for regulation and technical actions to solve the problem of lack of security awareness so that users can be aware of the security risks and enjoy the automated surveillance by IoT devices. Yuchen et al. (2017) explained that IoT devices have security gaps.

IV. Future IoT Developments

Ahlmeyer&Chircu (2016) opined that future research on IoT should include work on the economic, technical, and adoption barriers for IoT security practices, and the problems of security development and adoption. The duo indicated that future studies on IoT should involve incorporating security considerations into business model frameworks for IoT. Future work should also include identifying IoT security risks and building and implemented tested solutions to these risks (Ahlmeyer&Chircu, 2016). Saarikko, Westergren&Blomquist (2017) conducted a qualitative study on IoT's future. The researchers reviewed the advancement of the IoT and that of an increasingly interconnected environment, and the growing need to build partnerships to build innovative solutions. Kumar, Vealey and Srivastava (2016) indicated that for future studies, the items in the environment of the IoT could be connected with the proper authentication and authorization appropriate for the environment of the IoT with a quicker encryption contrasted with the techniques in existence; execution of cyber sensors to record data from physical articles to measure threat index so as to perform activities or real-time event feedback; recognizing the privacy prerequisites, privacy-related factors and the system to assess Threat Index for Privacy and shield IoT from privacy-related threats; Adjustment of the public key infrastructure to the environment of the IoT in the framework; Guaranteeing the physical level security issues, for example, physical altering and power denial assaults getdealt with; Creation of threat models for attacks such as Man in the Middle and Eavesdropping and assess threat index for such attacks and react to them in real-time; and Creation of techniques to guarantee secure IPSec and transport layer without relying on intermediate nodes so as to ensure total end-to-end security.Sathish Kumar & Patel (2014) explained that for future research and works on IoT, there are manyprivacy and security open issues and problems that should be solved to have a protected platform. Hsu & Lin (2016) indicated that future studies could increase the sample's diversity. Instead of using the Value-based Adoption Model as a theoretical model to examine user's intention to adopt, future research could also use other values such as performance, emotions, value-for-money, and social value to tests its influence on adoption. The research was also limited to Taiwan. But it serves as a motivation for future studies (Hsu & Lin, 2016). Weber (2015) opined that for future IoT works, he suggested the development of legal regulations for the protection of privacy. Borgia (2014) suggested nano-technology, nanoscale devices development, and innovative solutions that would tackle the modeling of the channel, encoding of information, and communication protocols for the integration of these nanodevices into IoT (Borgia, 2014). Yuchen et al. (2017) suggested the need for the development of robust security policies and standards for IoT devices and systems in the future.Andersson&Mattsson (2015) suggested that for future research on IoT, there may be further studies on service innovations that are IoT-enabled. Atzori et al. (2010) suggested that future studies on IoT, there should be an industrial applicable to IoTapplications. Balaji& Roy (2016) suggested that future research on IT could use qualitative study; examine the function of perceived embeddedness and power in affecting value co-creation and Continuance Intention of retail Internet of Things technology; and test their role invalue co-creation for Internet of Things.Bojanova et al. (2014) suggested that for future research on IoT, a global clock can be made original and that with Internet of Anything, anything can happen. Da Xu et al. (2014) suggested that IoT and cloud could be unified and that future research on this will focus on establishing platforms that will offer to sense asa service on the cloud. Hsu &Yeh (2016) opined that further studies could

use interviews to choose others for bringing balance to the conflicting aims. Future studies could also use the fuzzy extension of DEMATEL and significant group decision-making to compare to have insights for theessential determinants of success influencing IoT adoption (Hsu &Yeh, 2016).

V. Conclusion

There are factors, challenges and gaps affecting the adoption ofIoT. These factorsinclude technology readiness, compatibility, complexity, executive management support, firm size, regulatory support, security concerns, cost savings, compatibility and relative advantage and intention to adopt Internet of Things. The intention to adopt IoT and seven other factors were critically analysed. Other factors, challenges and gaps affecting IoT adoption, and future IoT developments were also analyzed. The findings of this research study could help Information Technology leaders and organizations to understand the factors that affect Internet of Things adoption, so that they can adopt and implement IoT.

References

[1]. Ahlmeyer, M., &Chircu, A. M. (2016). Securing the Internet of things: A review. Issues in Information Systems, 17(4), 21-28.
[2]. Alkhalil, A., Sahandi, R., & John, D. (2017). An exploration of the determinants for decision to migrate existing resources to cloud computing using an integrated TOE-DOI model. Journal of Cloud Computing, 6, 1-20, doi: 10.1186/s13677-016-0072-x
[3]. Andersson, P., &Mattsson, L. (2015). Service innovations enabled by the Internet of things. Industrial Marketing and Purchasing Journal, 9(1), 85-106. doi:10.1108/IMP-01-2015-0002
[4]. Atzori, L., Iera, A., &Morabito, G. (2010). The Internet of things: A survey. Computer Networks, 54(15), 2787-2805. doi:10.1016/j.comnet.2010.05.010
[5]. Atzori, L., Iera, A., &Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm. Ad Hoc Networks, 56, 122–140. doi:10.1016/j.adhoc.2016.12.004
[6]. Awa, H., Ojiabo, O., &Orokor, L. (2017). Integrated technology-organization-environment (T-O-E) taxonomies for technology adoption. Journal of EnterpriseInformation Management, 30(6), 893-921. doi:10.1108/jeim-03-2016-0079
[7]. Balte, A., Kashid, A., &Patil, B. (2015). Security issues in internet of things (IoT): A
[8]. survey. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 450-455.
[9]. Balaji, M. S., & Roy, S. K. (2016). Value co-creation with internet of things technology in the retail industry. Journal of Marketing Management, 33(1-2), 7–31. doi:10.1080/0267257x.2016.1217914
[10]. Bojanova, I., Hurlburt, G., &Voas, J. (2014). Imagineering an internet of anything. Computer, 47, 72–77. doi:10.1109/mc.2014.150.
[11]. Borgia, E. (2014). The Internet of things vision: Key features, applications, and open issues. Computer Communications, 54(1), 1-31. doi:10.1016/j.comcom.2014.09.008.
[12]. Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243.doi:10.1109/TII.2014.2300753.
[13]. Farooq, M., Waseem, M., Khairi, A., &Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). International Journal of ComputerApplications, 111, 1–6. doi:10.5120/19547-1280
[14]. Haddud, A., DeSouza, A., Khare, A., & Lee, H. (2017). Examining potential benefits and challenges associated with the Internet of Things integration in supply chains. Journal of Manufacturing Technology Management, 28(8), 1055-1085.doi:10.1108/jmtm-05-2017-0094
[15]. Hsu, C.L., & Lin, J. C. C. (2016). Exploring factors affecting the adoption of Internet of Things services. Journal of Computer Information Systems, 58(1), 49–57. doi:10.1080/08874417.2016.1186524
[16]. Hsu, C.W., &Yeh, C.C. (2016). Understanding the factors affecting the adoption of the Internet of Things. Technology Analysis & Strategic Management, 29(9), 1089–1102. doi:10.1080/09537325.2016.1269160
[17]. Hwang, Y.M., Kim, M. G., & Rho, J. J. (2016). Understanding Internet of Things (IoT) diffusion: Focusing on value configuration of RFID and sensors in business cases (2008-2012). Information Development, 32, 969-985. doi:10.1177/0266666915578201
[18]. Ives, B., Palese, B., & Rodriguez, J. A. (2016). Enhancing customer service through the Internet of Things and digital data streams. MIS Quarterly Executive, 15, 279– 297.
[19]. Ji, H., & Liang, Y. (2016). Exploring the determinants affecting e-government cloud adoption in China. International Journal of Business and Management, 11(4), 81. doi:10.5539/ijbm.v11n4p81
[20]. Krotov, V. (2017). The Internet of Things and new business opportunities. Business Horizons, 60(6), 831-841. doi:10.1016/j.bushor.2017.07.009
[21]. Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in internet of things: Challenges, solutions, and future directions. 2016 49th Hawaii International Conference on System Sciences (HICSS). doi:10.1109/hicss.2016.714
[22]. Martins, R., Oliveira, T., & Thomas, M. A. (2016). An empirical analysis to assess the determinants of SaaS diffusion in firms. Computers in Human Behavior, 62, 19– 33. doi:10.1016/j.chb.2016.03.049
[23]. Ng, I., & Wakenshaw, S. (2017). The Internet-of-Things: Review and research directions. International Journal of Research in Marketing, 34(1), 3-21. doi:10.1016/j.ijresmar.2016.11.003
[24]. Oliveira, T., Thomas, M., &Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. Information & Management, 51, 497–510. doi:10.1016/j.im.2014.03.006
[25]. Rosas, J., Brito, V., Palma, L., &Barata, J. (2017). Approach to adapt a legacy manufacturing system into the IoT paradigm. International Journal of InteractiveMobile Technologies, 11(5), 91. doi:10.3991/ijim.v11i5.7073
[26]. Saarikko, T., Westergren, U. H., &Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? Business Horizons. doi:10.1016/j.bushor.2017.05.010
[27]. SathishKumar, J., & R. Patel, D. (2014). A survey on Internet of Things: Security and privacy issues. International Journal of Computer Applications, 90(11), 20-26. doi:10.5120/15764-4454.
[28]. Shaltoni, A. M. (2017). From websites to social media: exploring the adoption of Internet marketing in emerging industrial markets. Journal of Business & IndustrialMarketing, 32(7), 1009–1019. doi:10.1108/jbim-06-2016-0122
[29]. Singh, G., Gaur, L., & Ramakrishnan, R. (2017). Internet of Things - technology adoption model in India. Pertanika Journal of Science & Technology, 25(3), 835-846.
[30]. Taneja, S., Pryor, M., & Hayek, M. (2016). Leaping innovation barriers to small business longevity. Journal of Business Strategy, 37(3), 44-51. doi:10.1108/jbs-12-2014-0145

[31]. Voas, J. (2016). Networks of things. NIST Special Publication 800-183.
[32]. doi:10.6028/NIST.SP.800-183
[33]. Weber, R. H. (2015). Internet of things: Privacy issues revisited. Computer Law & Security Review, 31(5), 618-627. doi:10.1016/j.clsr.2015.07.002
[34]. Weinberg, B. D., Milne, G. R., Andonova, Y. G. &Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. Business Horizons, 58(6), 615-624. doi:10.1016/j.bushor.2015.06.005
[35]. Yang, H., Lee, H., & Zo, H. (2017a). User acceptance of smart home services: an extension of the theory of planned behavior. Industrial Management & DataSystems, 117(1), 68–89. doi:10.1108/imds-01-2016-0017
[36]. Yuchen Y., Longfei W., Guisheng Y., Lijie L., &Hongbin Z. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal. 4(5), 1250-1258
[37]. Zhong, R. Y., Xu, X., & Wang, L. (2017). IoT-enabled smart factory visibility and traceability using laser-scanners. Procedia Manufacturing, 10, 1–14. doi:10.1016/j.promfg.2017.07.103