International Journal of Engineering & Technology, 11 (1) (2022) 14-19

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Key Factors Influence on Decision Making to IoT Adoption in Telecommunication Companies: A Review

Elham Abdulwahab Anaam [1*], Muhamad Naser Yousef Magableh [2]*, Ahmed Ridha Khudhur [3*], Sadoon Hussein Abdulallah [4]

[2] *School of Engineering and Technology, Central Queensland University, 4700, Queensland, Australia*
[3] *Universiti putra Malaysia, Communication Engineering, Malaysia*
[4] *College of Science, University of Mosul, Iraq*
**Corresponding author E-mail: anaamelham@gmail.com*

Abstract

In the context of the impact of advertisement IOT technology, the paper seeks to clarify the critical issues, specifically for telecommunication that deals with the novel technology but sometimes become complex because That is impacted by the constant changes in the information and communication technologies sector, that further leads to high operating expenses for organizations recent technological acquirement, installation, staff training for proper use of every new technology, and costly agreements to the Internet of Things suppliers for the implementation of IoT applications. The decision to adopt IoT technology will assist in predicting the best moment for a prominent telecommunications provider to deploy IoT systems, combining new mobile technologies and densifying its current network at an unmatched rate in the following years. Given the rising relevance of decision-making to IoT adoption and there is a lack of investigation and comparison of decision-making criteria with IoT platforms in this field. This article aims to provide four key factors that influence IoT adoption decision-making in a telecommunication company. Depending on the value of net theory, this article outlines four technical characteristics that influence decision-making in IoT adoption in a telecommunication company. The findings identification are the main factors for telecommunications companies to successfully token decision-making to IoT technology adoption.

Keywords: *Decision Making; IoT Adoption; Telecommunication Company; and Key Factors.*

1. Introduction

In the last decade, an enormous amount of data increased to exchange on the Internet. However, in the long term, the next generation of telecommunication is (5G), which deems and is gaining considerable momentum from both industry and academic research. With the development of the IoT, Internet-connected objects have recently acquired prominence (IoT). The (IoT) is part of the fundamental technologies of the Fourth Industrial Revolution. It refers to the gap connected to wired or wireless communication networks that may communicate data obtained through sensors without interpersonal interactions and complete preprogrammed tasks independently. Most products can now be networked, communicated with, accessed, saved, analyzed, and used. Smart homes, smart buildings, healthcare, and self-driving cars are technologies that can be implemented via IoT systems. This is about deploying business processes based on these theoretical frameworks or Internet of Things structures that provide layers, building relationships with technology, procedures, and devices among both organizations, considering demands. Proof of identity connection, interoperability, sympathetic connectivity, autonomic services delivery, and destination connectivity are just a few examples. Security, data confidentiality, excellent quality, and capabilities services relating to the human body are exceptionally secure, plug and play, and accessible [Gartner2017]. This screenplay demands the develop IoT project implementation methods that consider the following factors. The company's business model, as well as its personnel and financial resources, as well as the organization's technology resources. Furthermore, because the company's employees are unaware of the IoT potential, the employment of experts to help the IoT project from decision making through architecture is necessary. It is crucial to develop and implement projects to lower the program's risk (Gartner 2017). A previous academic researcher has paid attention to Lee & Lee (2015) monitoring, Big Data and enterprise statistics, and data sharing were studied as three IoT groups of real-world IoT systems that improve product quality. (Yu and Kim, 2019) investigate and contrast the security features of domestic and foreign IoT infrastructures in telecommunications firms. It is critical for a healthy environment; however, a significant impact on the economy has contributed value and created new jobs. Restrictions stemming from a lack of technology and financial resources. A lack the resources and skilled employees to prevent them from being successful. In the marketplace, you must be competitive (Ivanschitz 2015). The (IoT) is a technology movement altering business practices and can be viewed as a marketing opportunity for telecommunication businesses. Firms must use digital technology to better their marketing strategies Innovation (Choi2015). IoT adoption proposes a challenge for telecommunication companies to attain a wide range of technical sophistication planning. Not just that, but it's being created with compatibility with a range of devices in mind. Nonetheless, however, the domestic market remains stagnant. IoT platforms are thought to have a lesser level

of security compared to global IoT platforms. Even though this issue is well-known, there is a lack of investigation and comparison of decision-making criteria with 5G with IoT platforms. Furthermore, because each of the present Interfaces for IoT on a global scale was built individually, security for interoperability was not given enough consideration. As a result, in this article, we examine and evaluate the decision-making aspects of domestic and international IoT platforms and predict future IoT platform directions. The Contribution in the current study scanning the previous literature review of the related scope of study with IoT and 5G. (Mistry et al., 2020) discuss blockchain-based industrial automation for the applications. (Miraz et al. 2018) Evaluate blockchain Existing security effectiveness. (Dorri et al. 2016) suggested secure and flexible IoT technology. (Hwang et al.2018) suggest a method to direct connection among devices. But the contribution of the current study is:

1) Using decision-making to identify critical issues in the adoption of IoT in telecommunication companies.
2) There are no studies that have attended the potential of decision making to integrate IoT with 5G for identifying challenges of successful adoption in telecommunication companies.

2. Literature Review

2.1. Related Work

Publications regarding IoT adoption published between 2016 and 2019 were located in the research and use the relevant descriptive terms: “IoT” stands for Internet of Things. Abazi (2016) described the procedure that small and medium businesses must follow when making IoT adoption decisions, stating which owners, administrators, and staff members should be knowledgeable about the Internet of Things and its effect on the company. The author mentioned two factors to be considered when implementing IoT. Nylander, Wallberg, & Hansson (2017), The researchers conduct an interdisciplinary study (partnership between computer science, business model studies, and process improvement research), concluding that to adopt Internet of Things solutions, the company must first obtain technological expertise. Additionally, Actions in the IoT sector are required to solve standardization, accessibility, and security issues. Lee (2019) presented an IoT ecosystem, IoT architecture, and the IoT service business model required for the deployment of IoT services in enterprises.

2.2. Evolution Internet of Things (IoT)

Besides using the phrase alone, modern components of IoT have been merged into several different technologies, with popular definitions based around the Internet of Things. Sensory network of true or real items. Observation and collaboration with other companies (Ali Dorri et.al 2016). There are approximately 5 billion smart devices globally, which helps people understand the rise of the Internet of things and its worldwide scope. It is estimated that over 50 billion devices will be sold. By 2020, smart devices connected to the Internet will be the norm (DongYeop et.al 2018). This statistic is cited across several academic studies with multiple layers of references, yet the source of this data is a journal article. Ericsson issued a study in February 2011, the largest telecommunication corporation that specializes in networking. The original document makes it crystal evident that the expected outcome will occur. An estimate of 50 billion connected smart devices by 2020 was given. Just an attainable objective and somewhat imaginative becoming a representation instead of an accurate prognosis, a risk-averse person may find a forecast or supposition to be an obstacle organization. Regardless of Ericson's mass volume ideas from 2011, the growth of connectable or smart IoT devices can be found in many aspects of life around the globe. Spanning from security systems to refrigerators and everything in between factories that are highly automated and coordinated. The following visions can explain the integration of IoT into three common organisms: "Things oriented," for example, sensors, "Internet-focused," for example, the Internet, and "semantically focused" for limit access (Mahdi 2018).

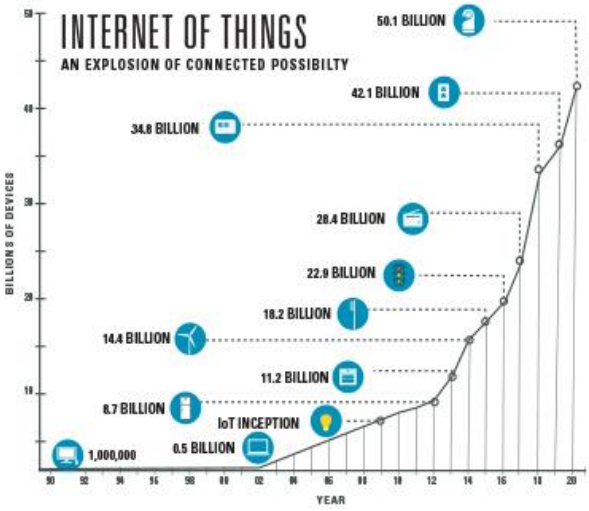


Fig. 1: Growth in the IoT.

2.3. Businesses and Developments in The IoT Platform

Moore (1993) proposes that a company be considered as part of a business ecosystem that spans many industries rather than as a particular sector. In general, ecosystems feature either a hub-centered star shape or a flat mesh-like structure (Mazhelis et.al 2012). The top framework is found in west, where IoT ecosystems are built around main IT companies like Google, Amazon, Facebook, and Apple that interact with a large number of small businesses, whereas the flat mesh-like framework is discovered in the European Union, where the IoT environment is made up of small and adaptable businesses (Kubler2013). An business environment enables businesses to collaborate and compete with one another to promote new components, grow marketplaces, and boost productivity. An Iot application network, according to (Mazhelis et al.2012) is a specific type of business ecosystem made up of cooperating IoT-related enterprises and individuals, as well as their socioeconomic surroundings. They propose that technology platform vendors, hard-ware network operators, and regulatory requirements comprise the community of an IoT ecosystem. Cross-industry players can output metrics to a business Iot network [14]. Because most Cloud platforms necessitate the integration of several devices and software modules from various vendors, most businesses lack the technical expertise required to provide the necessary assistance. Considering the smart Iot environment will aid in the selection of the appropriate Iot networks for service improvement.

Table 1: The Application of the Internet of Things (IoT) Access

1	Model: Key Decisions: Improve the customer experience, provide a more economical hotel accommodation, and contributing to Marriott's global sustainability performance and objectives.	Customers would enjoy an integrated experience with access to their own data and information
2	Collaboration: Form a relationship with Samsung and Legrand. Samsung uses the ARTIK platform and the SmartThings Cloud to create an end-to-end IoT service that includes everything from intelligent illumination to voice-activated room controls. Legrand provides a range of power, light, and data solutions that provide electricity and communication to previously inaccessible area.	Security, authentication, and access management from beginning to end. Platform allows Alexa from Amazon to "speak" to IoT devices (e.g., thermostats and lights in hotel rooms).
3	Hotel takes advantage of VMware's latest extending of its IBM Cloud collaboration. Provider IT paradigm that would enable a	A cloud platform that is virtualization, application, and

variety of new digital experiences by safely extending towards on data centre into the cloud platform.	controlled

2.4. Characteristic of IoT

The three elements of IoT communication firms are perceptive layer, network layer, and application layer systems (YAN Bo et al. 2009). It serves as a platform for IoT to detect objects and gather data. The presentation layer serves as a link for IoT and users (including man, organization, and other systems). It interacts with industrial requirements to meet the smart use of IoT (Liu Yujie, 2009). The architecture of IoT is seen in Figure 2. The major purpose of the network layers is to gather and process information, while the expansion layer is made up of typical wireless sensor networks, Radio Frequency Identification, RFID, and the ultimate controlling mechanism are all part of the WSN system. The network layer includes two dimness bar codes that identify the device, RFID labels, camera gaps' sensor, m2m terminal, a portable terminal, sensor network, and sensor portal. The IoT network layer is built on top of today's mobile telecommunications and internet infrastructure (Yang, Zhihong. Et.al 2011). Its primary function is to transmit data over a great distance.

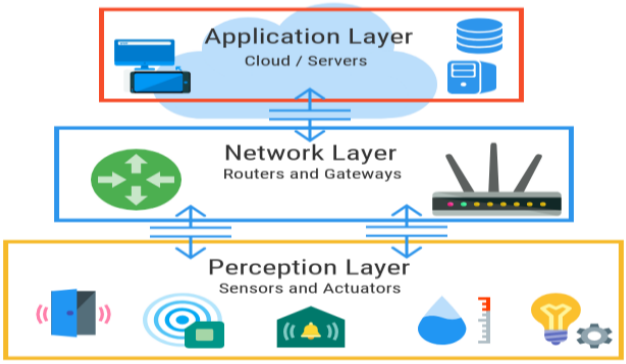


Fig. 2: Characteristic of IoT.

2.6. Challenges

IoT and its use in many sectors are increasing at an exponential rate over the recent years. YAN (2009) there are enormous data of IoT-enabled devices, more than 20 billion, by 2020. This big data need to manage adequate storage, and processing approaches. (Mistry et al., 2020) stated that The IoT has Technology was used to modify these circumstances, in which the challenges as mentioned earlier may be addressed by direct contact between robots, data, and humans. Moreover, (Anaam .et.el 2021). Mentioned that the failure of signal points and lack of trust between sharing systems are the main issues of IoT. (Mistry et al., 2020) to control the IoT limitation can be used per-peer communication between nodes. But this type of connection of system has several concerns like privacy and security that can be open the door for hackers. Moreover (Shah, Bolton, and Menon, 2020) Access to particular data exchanges and increasing collaboration, trust is a vital key element for successful (IoT) adoption. This fundamental review of a few of the issues and risks of (IoT) in telecommunication companies is only a taste to pique your interest as technology advances, prompting further investigation into future consequences.

2.7. Research Gaps

This article focuses on examining decision-making ideas concerning IoT adoption and its broader applicability across the global E-CRM (Anaam, Azmi, et al., 2020). Within the literature investigated, the scholar has recognized some of the influences and challenges on IoT adoption in worldwide E-CRM(Anaam et al., 2018), which will also assist industries and other scholars who are evaluating developing further while implementing IoT within telecommunication companies(Anaam, Abu Bakar, et al., 2020). Despite the great awareness and disruptive nature of IoT in E-CRM, the highlighted hurdles and concerns, in contrast to the few applications and unknown advantages, highlight the initial phase of IoT in E-CRM.

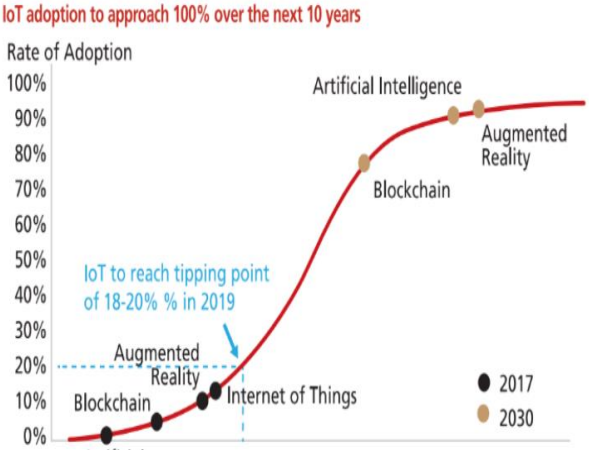


Fig. 3: h 1oT Adoption Source:(Shah, Bolton and Menon, 2020.

3. Methodology

3.1. Searching Process in Databases

The examination method of this literature involves collecting databases from the thesis, journals, and conferences with keywords. The databases were selected for the years from 2000 to 2020. The databases used are as shown in Table 1. This study selects journals and conferences based on these keyword queries (Decision making, IoT adoption, telecommunication company, and Key factors). The database collection provides an important list of possible researches. The processes in selecting the studies relevant to paper review are as follows:

1) Exclude studies whose titles are not relevant to the paper goal.
2) Exclude papers with their abstracts and keywords not related to the paper goal.
3) Read the remaining sections on the papers and exclude any paper that is not relevant to the scope.

3.2. Identify Literature Review

This study aims to do a previous literature Analysis to find the most critical factors to take decision making to IoT adoption that contributed optimistic about successful adoption of IoT systems. In telecommunication companies. The study Ues different keywords such as Decision making, IoT adoption, telecommunication company, and Key factors.

3.3. Identify Value Net Theory in Telecommunication

Telecom companies have considerable cost convergence capability in the IoT value net. They may extract knowledge and capabilities from members in the IoT chain, making them important hubs in the series. When the value net generates interests, telecommunications firms act as a link between participants. In the value net, they are therefore organizers and organizers. Based on the integration, the IoT network is costly and takes decision making to adopt as this networking needs to employ high skills (Qin et al. 2015).

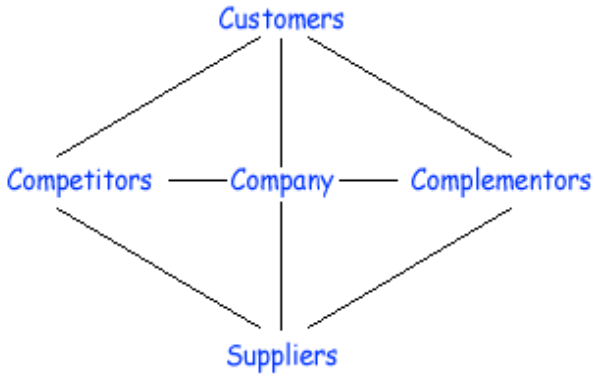


Fig. 4: Value Net Theory.

4. Results

4.1. Main Factors of Decision Making to Adopt IoT In Telecommunication Company

There are different factors to make decisions to adopt IoT that have to consider, such as platform providers, item providers, security, Cost, employee skills, an environment of IoT, and customers (Ziegeldorf 2014). Based on the analysis in a literature review. This paper identifies four critical factors of decision-making to adoption IoT in a telecommunication company. When the value net generates interests, telecommunications firms act as a link between participants. In the value net, they are therefore organizers and organizers. The integration of the IoT network is costly and takes decision-making to adopt as this networking needs to employ high skills. Customers can purchase IoT goods and services from telecom providers. They can understand consumers' demands and report back to them in real-time since they have a huge customer base and direct touch. This will enable them to respond to market demand fast like customers and participants.

a) Security
b) Cost
c) technology developers such as telecom companies, connectivity platform developers, data network developers.
d) Users and customers (corporate users, corporate customers, individual customers).

These critical factors contribute to the success, expand markets, facilitate communication and competition in the companies, and benefit enterprises, users, and customers. Fig. 6 presents the key players of the adoption of IoT.

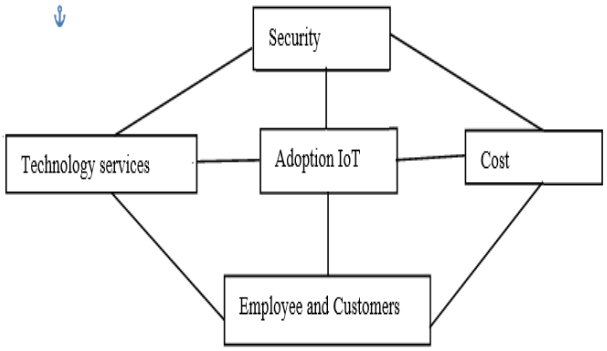


Fig. 5: Key Factors to Decision Making to Adopt IoT.

4.2. Technology Services

The blockchain is used for emerging technology. The transition is essential to a decentralized, cryptographically secure Network between a centralized customer service online platform. Furthermore, the blockchain is essentially an unchanging leader that can confirm banking transactions. It helps customers have a transmitted P2P network in which non-trustworthy members can share information without needing a secure intermediary (Gartner 2018). Trust and security are key features of blockchain that can be accomplished by using the resulting previous blocks. To reach a consensus, the obtained hash is validated by nodes and then found the secret key for the following block. This process is termed the Proof-of-Work (POW), and the mineral clusters are recognized for the work carried out in the system (Chellappan 2016). Such motivation models encourage the mining clusters to participate in the network to communicate computer power for mining blocks. In addition, Blockchain differs in consensus and continues to follow properties from other sensor networks. The following are the following: Trust-less, Permission-less, Censorship resistant. In addition, Technology Blockchain technology services have main aspects as (a) Consensus: The PoW protocol is verifying all activities in the network extremely important to prevent a possible miner node controlling the whole blockchain network and manipulating the record of transactions. (B)Cryptography: It provides strong authentication encryption across all data of the network. (c) Smart Contract: It only enables legitimate access to encrypt information. Different types of blockchain technology services can be distributed on essential parameters, successes data, availability, and arrival control. The variation lies in the notion of authentication, which mentioned who can arrive at the blockchain technology services (audience vs. private) and allowance, which points out what the participant could do (permission vs. non-permission). In the case of audience blockchains technology services, anybody can participate in the network, regardless of any type of agreement. While, in private blockchains technology services, sharing is limited, where the owner's agreement is needed to access the network.

4.3. Security

To establish an Internet of Things solutions in enterprises (telecommunications companies), security threats to data and service privacy, authenticity must be addressed (V. Chellappan et al. 2016). Among the most severe effects of weaknesses is the loss of an organization's reputation (for example, through compromising client privacy), resulting in costly legal action (J. H. Ziegeldorf et al. 2014). According to Gartner, firms worldwide will spend $3.1 billion on Security issues in 2021 to prevent themselves from IoT-based attacks (Gartner 2008). Notwithstanding their budgetary constraints, telecommunication companies must think about investing in IoT security. Considering the IoT reference model described in Guideline ITU-T Y.4000/Y.2060, which integrates security capabilities categorized into two categories (Anaam et.al 2018), this is one of the obstacles for the performance of IoT projects from R&D activities. General security capabilities (independent of applications, included in the application, network, and device layer, such as permissiveness, authentication, incoming monitoring, data privacy, device safety validation) and specific security abilities (connected to the application-particular demand and mobile payment). Furthermore, the IoT development player will likely employ the necessary papers to ensure the security and privacy of the IoT solution's characters: (1) ITU-T Recommendations X.1205: Fundamentals of Cybersecurity (Anaam et. al 2020), which gives a taxonomy of the security dangers which can harm an organization. (2) ITU-T Y.4806: Security capabilities enhancing Internet of Things security; outlines security issues that could influence Internet of Things security and safety capabilities. (ITU-T 2017). According to Lee & Lee, a lack of safety and privacy may be leading to the failure of IoT adoption projects (I. Lee and K. Lee 2016). One approach to transact with this issue is regarding the employee skills of IoT professionals to deploy obtain settlement depending on R&D activities. In this regard, the CIO is expected to work closely with the CISO to guarantee that competent people with IoT security expertise are included in the IoT development team and the purchasing of IoT devices and software solutions to install safe IoT applications (Gartner, 2018). Telecommunication companies must ensure the creation of IoT solutions with robust security to confront cyber-attacks and have difficulty hiring

personnel with IoT security capabilities. Three major kinds of risks influence Internet of Things solutions. (Chellappan et al. 2016). Take a picture (is accountable for catching information), tamper, which relates to refusing, destroying, and interrupting the IoT solution, and Disrupt (refusing, destroying, and disturbing the IoT solution related to data manipulation. Passive threats (snoop or transmission monitoring) and active threats (attacking the Internet of Things network) are both possible risks (misrepresentation, man-in-the-middle, re-enactment) Denial-of-Service (DoS) assaults).

4.4. Cost

The cost of deploying the Internet of Things varies greatly due to the use of traditional research methods and techniques of communication (e.g., Internet, e-mail, website, e-Commerce, e-CRM) in terms of their degree of difficulty. To decrease project risk, the CIO must consider Factors related to technology, organization, and the environment (technological infrastructure, technological support, research and development activities, IoT managers skills, IoT skills of employees, behavioral intention to use Internet of Things, sector, firm size) Calculate an estimated investment cost defined by two scenarios. (1) The Internet of Things project will be combined with current information and communication technologies to improve them, such as e-Commerce and E-CRM (H. Yu and X. Zhang, 2017). or promote the implementation of numerous alternatives in the company, considering technology developments such as Cloud Computing (A. Botta et al. 2016). (2) The Internet of Things (IoT) project is a new technical solution based on the Internet of Things that necessitates technical preparedness to support the digitalization of the business to enhance procedures, goods, or activities. Including both situations, positive results from prototypes or perhaps even pre-test are anticipated to validate IoT expenditures in the initial phases of IoT adoption because the cost to install IoT solutions is typically greater than projected. Among all the costs that telecommunication company businesses should bear to complete IoT, initiatives are the following: employ experts of the employee's in the Internet of Things (from various fields of a specialist such as Computer Science, Engineering, Decision Sciences, Social Sciences, Energy, Business, Management, and Accounting), with high skills to share in technological innovation processes; training staffs for the conquest of new digital skills to go ahead with the digital processing for the appropriate use of factors IoT trends and technologies such as offering courses relevance basic competences of IoT, improve security skills, analysis data, hardware and software support.

4.5. Employee and Customers

Employees and consumers receive IoT-based services from businesses to enhance their business processes and customer needs. Employees and consumers are the benefactors and income generators who support IoT development going ahead. Optimizing machine maintenance, locating ships and trucks, aiding consumers with shopping, achieving efficiency in checkout processes, and controlling workplace security and electricity costs are just a few of the ways IoT helps employees and consumers (C. Bardaki et al. 2012; S.H. Choi et al. 2015; H. Evanschitzky et al. 2015). Employees and consumers must adopt IoT services for the IoT investments to fully utilize. According to a new analysis, perceived utility and enjoyment of IoT services favorably influence behavior in utilizing IoT services but perceived privacy risk negatively impacts IoT adoption (C.-L. Hsu et al. 2018).

5. Conclusion

The deployment of IoT business will assist the digital revolution in telecommunication companies. services (IoT technologies together) and business applications) will be headed primarily by the (assigned as the project manager for the IoT projects). who should deal with the framework's difficulty in light of three factors: technical, organizational, and environmental) Since the Internet of Things is such a new phenomenon, there are several studies on corporate IoT. This makes it difficult for businesses to make well-informed judgments on IoT quality improvement. This research addresses existing gaps that incorporate IoT study and aims to pique the curiosity of anybody concerned to incorporate IoT studies and practice in this field. This research highlighted key factors that contribute to decision-making to IoT adoption in telecommunication companies, such as security, cost, employee skills, and customers and technology services for support successful IoT service's needs. The factors play a significant role for IoT adoption, who will realize the planning to minimize business security, considering the limitation that refuses the growth of telecommunication company such as a lack of cost capacity, lack of ICT infrastructure, lack of IoT awareness). The IoT businesses group will include professional experts from various fields to propose enhancing the processes and improving security issues in IoT. The CEO's choice on IoT adoption in a telecommunications business is based on his innovative behavior. Prior expertise and understanding of the Internet of Things such as e-Commerce- e-CRM Cloud Computing.

References

[1] Yan, B., & Huang, G. (2009, August). Supply chain information transmission based on RFID and internet of things. In 2009 ISECS International colloquium on computing, communication, control, and management (Vol. 4, pp. 166-169). IEEE. https://doi.org/10.1109/CCCM.2009.5267755.

[2] Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011, July). Study and application on the architecture and key technologies for IOT. In 2011 International Conference on Multimedia Technology (pp. 747-751). IEEE.

[3] Parra, D. T., & 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.

[4] Lee, I., & 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.

[5] Miraz, M. H., & Ali, M. (2018, August). Blockchain enabled enhanced IoT ecosystem security. In International conference for emerging technologies in computing (pp. 38-46). Springer, Cham. https://doi.org/10.1007/978-3-319-95450-9_3.

[6] Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

[7] Hwang, D., Choi, J., & Kim, K. H. (2018, October). Dynamic access control scheme for iot devices using blockchain. In 2018 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 713-715). IEEE. https://doi.org/10.1109/ICTC.2018.8539659.

[8] Anaam, E. A., Bakar, K. A. A., & Satar, N. S. M. (2020). A Model of Electronic Customer Relationship Management System Adoption In Telecommunication Companies. Amazonia Investiga, 9(35), 61-73. https://doi.org/10.34069/AI/2020.35.11.5.

[9] Bardaki, C., Kourouthanassis, P., & Pramatari, K. (2012). Deploying RFID-enabled services in the retail supply chain: Lessons learned toward the internet of things. Information Systems Management, 29(3), 233-245. https://doi.org/10.1080/10580530.2012.687317.

[10] Choi, S. H., Yang, Y. X., Yang, B., & Cheung, H. H. (2015). Item-level RFID for enhancement of customer shopping experience in apparel retail. Computers in industry, 71, 10-23. https://doi.org/10.1016/j.compind.2015.03.003.

[11] Evanschitzky, H., Iyer, G. R., Pillai, K. G., Kenning, P., & Schütte, R. (2015). Consumer trial, continuous use, and economic benefits of a retail service innovation: The case of the personal shopping assistant. Journal of Product Innovation Management, 32(3), 459-475. https://doi.org/10.1111/jpim.12241.

[12] Yu, H., & Zhang, X. (2017, July). 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) (Vol. 2, pp. 434-436). IEEE. https://doi.org/10.1109/CSE-EUC.2017.269.

[13] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (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.

[14] Chellappan, V., & Sivalingam, K. M. (2016). Security and privacy in the Internet of Things. In Internet of Things (pp. 183-200). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-805395-9.00010-1.

[15] Anaam, E. A., Khairul, A., Abu Bakar, N. S., & Mohd, S. (2018). A theoretical review of conceptual model for E-CRM success in telecommunication companies. https://doi.org/10.14419/ijet.v7i4.17674

[16] Ziegeldorf, J. H., Morchon, O. G., & 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.

[17] El-Haii, M., Chamoun, M., Fadlallah, A., & Serhrouchni, A. (2018, October). Analysis of cryptographic algorithms on iot hardware platforms. In 2018 2nd Cyber Security in Networking Conference (CSNet) (pp. 1-5). IEEE. https://doi.org/10.1109/CSNET.2018.8602942.

[18] Parra, D. T., & Guerrero, C. D. (2020, June). Decision-making IoT adoption in SMEs from a technological perspective. In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE. https://doi.org/10.23919/CISTI49556.2020.9141045.

[19] Chellappan, V., & Sivalingam, K. M. (2016). Security and privacy in the Internet of Things. In Internet of Things (pp. 183-200). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-805395-9.00010-1.

[20] Lee, I., & 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.

[21] Anaam, E. A., Abu Bakar, K. A., Mohd Satar, N. S., & Ma'arif, M. Y. (2020). Investigating the Electronic Customer Relationship Management Success Key Factors in the Telecommunication Companies: A Pilot Study. Journal of Computational and Theoretical Nanoscience, 17(2-3), 1460-1463. https://doi.org/10.1166/jctn.2020.8825.

[22] Anaam, E. A., Azmi, K., Bakar, A., Safie, N., & Satar, M. (2018). Critical success factors for electronic customer relationship management success adoption: Telecommunication companies case study. International Journal of Advanced and Applied Sciences, http://science-gate.com/IJAAS/Articles/2021/2021-8-10/1021833ijaas202110013

[23] Anaam, E. A., Khairul, A., Abu Bakar, N. S. & Kamrul, M. (2021). Critical success factors for electronic customer relationship management success adoption: Telecommunication companies case study.

[24] J. Moore , Predators and prey: a new ecology of competition, Harv. Bus. Rev. 71 (3) (1993) 75–86 .

[25] O. Mazhelis , E. Luoma , H. Warma , Defining an Internet-of-Things ecosystem, in: S. Andreev, S. Balandin, Y. Koucheryavy (Eds.), Internet of Things, Smart Spaces, and Next Generation Networking. ruSMART 2012, NEW2AN 2012, Springer, Berlin, Heidelberg, 2012 Lecture Notes in Computer Science, Vol 7469. https://doi.org/10.1007/978-3-642-32686-8_1.

[26] S. Kubler , J. Robert , A. Hefnawy , K. Främling , C. Cherifi, A. Bouras , Open IoT ecosystem for sporting event management, IEEE Access 5 (2017) 7064–7079. https://doi.org/10.1109/ACCESS.2017.2692247.

[27] Shah, S., Bolton, M. & Menon, S. 2020. A Study of Internet of Things (IoT) and its Impacts on Global Supply Chains. Proceedings of International Conference on Computation, Automation and Knowledge Management, ICCAKM 2020 245–250. https://doi.org/10.1109/ICCAKM46823.2020.9051474