# Conceptualizing IoT-based Smart Campus Adoption Model for Higher Education Institutions: A Systematic Literature Review

Radhwan Sneesl
*Faculty of Computer Science and Information Technology*
*Universiti Putra Malaysia*
Malaysia
radhwan.sneesl@gmail.com

Yusmadi Yah Jusoh
*Faculty of Computer Science and Information Technology*
*Universiti Putra Malaysia*
Malaysia
yusmadi@upm.edu.my

Marzanah A. Jabar
*Faculty of Computer Science and Information Technology*
*Universiti Putra Malaysia*
Malaysia
marzanah@upm.edu.my

Salfarina Abdullah
*Faculty of Computer Science and Information Technology*
*Universiti Putra Malaysia*
Malaysia
salfarina@upm.edu.my

2022 Applied Informatics International Conference (AiIC) | 978-1-7281-8428-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/AiIC54368.2022.9914033

***Abstract*—The concept of a smart campus is still emerging, which sometimes refers to smart education that allows the applications of smart technologies in higher education institutions. This study focuses on how to leverage technology acceptance theories to promote the concept of smart campuses adoption. Therefore, the aim of this paper is to present a solution to address the lack of a technology adoption model for IoT-based smart campuses, which is limiting wide-scale implementation and usage. A systematic process was used to select relevant articles from the three reputable databases. The findings of the study revealed various limitations and challenges concerning the adoption of a smart campus. Also, the study discussed the theoretical technology adoption models used for IoT adoption. Hence, a conceptual model for the adoption of the smart campus was derived through the lens of a value-based adoption model (VAM). The model's components include propagation, perceived fees, perceived trust, and perceived value. The study offers practical and theoretical implications since the IoT and smart devices are still emerging, and more importantly, the smart campus concept is in its infancy.**

***Index Terms*—Smart campus, IoT, Adoption Models, VAM**

## I. Introduction

The advent of technology such as IoT and smart devices has required higher education institutions to modernize the traditional system of teaching and learning. Education comes to be known as a critical element in empowering people and encouraging them to take a more active role in smart city initiatives [1]. Smart devices have proven to be effective in a variety of applications as well as an educational environment through smart classrooms and mobile learning. The emergence of smart classrooms at the higher level of education is associated with urban smartness [2], and cities cannot "achieve smartness without talent, education, awareness, and learning" [3]. With such tremendous growth in the usage of smart technologies, many universities are piloting or considering adopting smart technologies in their campuses, which give birth to smart campuses [4].

For example, reference [5] conducted a comprehensive survey about universities that have implemented smart campus initiatives in Malaysia, which covers Universiti Putra Malaysia (UPM), Universiti Tun Hussein Onn Malaysia (UTHM), Universiti Tenaga Nasional (UNITEN), Universiti Malaya (UM), and Universiti Malaysia Pahang (UMP). The study revealed that the majority of the institutions had implemented some part of smart campus technology such as smart management, smart learning, green campus, smart healthcare, smart governance, and smart community. Remarkably, the smart campus initiatives were seen more in smart management with an example such as smart administration, smart transportation, smart student, cashless solutions, student information system, academic management, facility management, security solutions, smart mobility, smart security, and smart lifestyle. However, there is still no clear perception of what a "smart campus" would look like or the main components that can form a smart campus [6]. Similarly, reference [4] highlighted that a generic model to be used for the smart campus had not been established.

### A. Problem and Motivation

The implementation of IoT-based smart campus technology and framework cannot be successful without studying the adoption factors at the time of the release of the technology, to forecast future usage of that technology [7], which are lacking in the technology adoption literature, and a major hurdle to get benefits is adoption and use of any technology [8]. Hence, the lack of technology adoption models for the smart campus is limiting wide-scale implementation and

978-1-7281-8428-9/22/$31.00 ©2022 IEEE

usage. Thus, this problem has called for more research to add knowledge concerning the adoption of IoT-based smart campuses to help technology manufacturers, university administration, and policymakers understand the key determining factors for the successful adoption of such systems and their value. Understanding adoption factors could drive widespread IoT-based smart campus deployment. Hence, this study aims to bridge this gap by conceptually introducing the IoT-based smart campus adoption model.

### *B. Study Organization*

The study is divided as follows; section II discussed the literature review, section III explained the methodology, section IV discussed the conceptual model, section V covered concluding remarks.

## II. Literature Review

The phrase ”smart campus” refers to the combining and applying smart technology (IoT device) with infrastructural facilities in order to significantly improve service, decision-making, and sustainability in higher education institutions [4]. Smart campuses encompass a wide range of technologies, including smart classrooms, student attendance by smart card, smart grids, and infrastructure monitoring, all of which fall under the umbrella term. The IoT is considered to be the most significant enabler of smart campuses, surpassing both artificial intelligence (AI) and robot systems [9]. A huge advancement in information technology has occurred with the IoT, which has the potential to improve speed and ease in everyday life. The IoT is viewed as a potential means of merging numerous technologies to improve efficiency and quality of life [10]. Many IoT service users have increased widely, but little is understood about what motivates the continued use of such services [11].

Hence, this study reviewed the existing studies to identify current issues and challenges facing IoT smart campus solutions. The nature of IoT deployment raises concerns about privacy, security, and trust [9], [12]. Most significantly, security and privacy have indeed been identified as the most significant impediment to the growth of the Internet of Things [12]. The findings of the reference [13] study demonstrated that privacy and security issues have an impact on the intention to use the Internet of Things. Hence, the IoT issues and challenges described in the literature [14] are summarized in Fig. 1. Furthermore, the question of trust is considered to be complex [15]. Although there is no universally accepted definition of trust, it is commonly acknowledged as being crucial in the field of information systems [16].

In addition, the concept of trust is associated with the concepts of reputation and dependability [17]. Trust has two properties, according to the research, which are trust in the interaction between entities (users) and trust in the system from the users' point of view [18]. Accordingly, trust is essential when it comes to adopting and deploying IoT [9]. According to the paradigm developed by [19], trust should be considered throughout the entire IoT development process. At the same time, reference [20] suggested trust computing models that provided future study directions in the field of trust computation.

Similarly, the absence of a widely accepted research approach that connects current theories, models, or frameworks is essential for robust validity [21]. As a result, more predictors such as culture, lifestyle, social influences, personality, and cost are lacking to increase the adoption rates. The majority of the studies are not applied to IoT integrated university settings and so do not contribute to promoting the concept of smart universities or smart campuses. Hence, there is still no clear perception of what a smart campus would look like or the main components that can form a smart campus [4], [6]. Therefore, Fig. 1 presents typical issues and challenges as security concerns for the smart campus. Accordingly, the literature study has revealed that the technology adoption model (TAM) is the most applied theory for the adoption of IoT [22], [23], as presented in Fig. 2. However, the strength and limitations of the technology acceptance theoretical models are available in many disciplines, although the literature concerning the adoption of IoT smart campuses is still emerging.

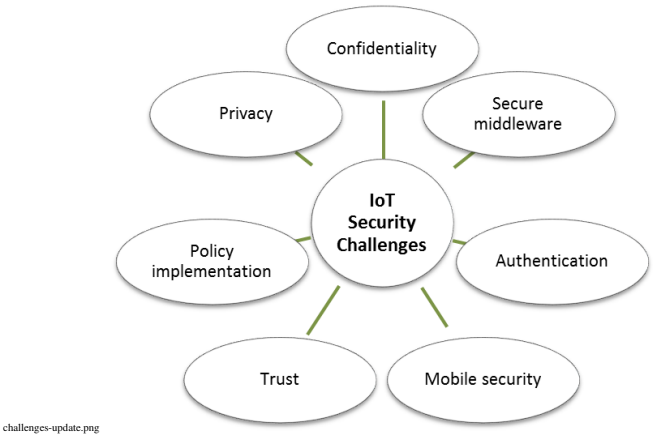



Fig. 1. Smart Campus IoT Security Challenges [17]

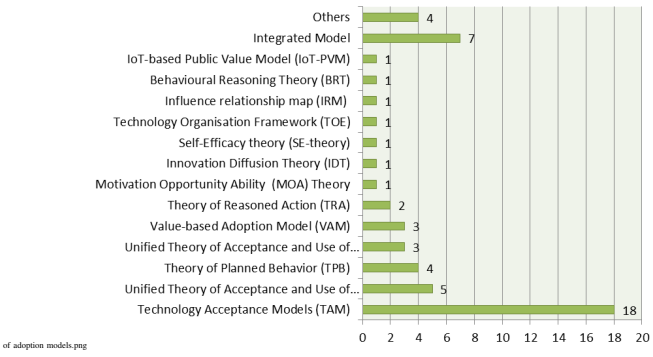
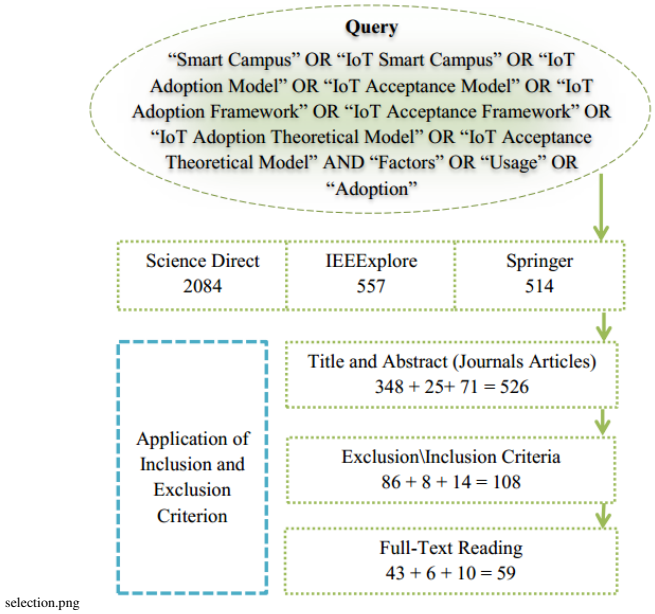



Fig. 2. The Frequency of Articles Published from 2016 – 2021

## III. Methodology

This study identified relevant research through a systematic literature review (SLR) approach applied in previous studies [24], [25]. One of the reasons for choosing this method is that SLR is essentially concerned well with the challenge of gathering empirical evidence, has a very well procedure that minimizes literature bias, and can provide relevant evidence about coherent and incoherent results across a wide range of empirical methods, among other things. Therefore, reputational online databases were visited (see Fig. 3). Articles are downloaded, and the inclusion and exclusion criteria are applied during filtration. Furthermore, the eligibility of selecting papers for this study was applied.

Furthermore, as depicted in Fig. 3, the SLR is divided into four (4) distinct stages. The SLR begins with searching for relevant articles, which is the first stage. In order to find research publications, a query is developed based on keywords discovered in the literature and entered into a search engine. For example, ”Smart Campus” or ”IoT Smart Campus” or ”IoT Acceptance Model” or ”IoT Adoption Framework” or ”IoT Acceptance Framework” or ”IoT Adoption Theoretical Model” or ”IoT Acceptance Theoretical Model” and ”Factors” or ”Usage” or ”Adoption” are some of the keywords. Specifically, the search query retrieved 2084 items in Science Direct, 557 articles in IEEExplore, and 514 articles in Springer, in that order. In the second stage, the publications were filtered based on their titles and abstracts. Articles that were not linked to the topic of the research were not taken into consideration throughout this stage of the process. The articles that were chosen for further evaluation were subjected to additional inclusion and exclusion criteria as part of the process. Conference papers, non-English text, and non-open access articles are among the exclusion criteria. In contrast, index JCR or Scopus papers, as well as studies that adopted or adapted technology adoption theories in the research design, are among the inclusion criteria. So the final sample consists of 108 articles, all of which will be considered for full-text reading in the last stage of this process. As a result, 59 publications were chosen as final study samples since they met all of the final eligibility criteria, as depicted in Fig. 3. Thirty-one papers are based on technology adoption theories for Internet of Things devices across a wide range of application domains. Twenty-eighty papers focus on technologies enabling smart campuses.



selection.png

Fig. 3. Search and Selection Process

## IV. Smart Campus Adoption Model

According to the reference [26], many people are critical of technology adoption models such as TAM because they do not take into account behavioral intention derived from complicated interactions incorporating earlier use views. The general factors of TAM (usefulness and ease of use), as described by [27], are insufficient for describing a complex situation since the variables do not take into consideration users' existing associations with the system. The TAM model is straightforward and strong, but it has the disadvantage of excluding potential variables that may be significant [28]. Many literatures have disputed the assumption of the link between intention and actual action, stating that it cannot ensure real use [28], [29]. The second point of contention is that the TAM constructs are weak because of a lack of explanatory power and inconsistencies amongst them, as stated in reference [30].

In a similar vein, the unified theory of acceptance and use of technology (UTAUT) concept places emphasis on diverse technologies while neglecting to justify the users' expectations and beliefs that are likely to arise as a result of utilizing the technology [31]. Furthermore, UTAUT places a greater emphasis on expectation performance than it does on personal expectation. As a result, the UTAUT paradigm is best suited for use in the workplace rather than in public settings. Despite the fact that several studies have contributed to the prediction of intention and behavior using the UTAUT model [26].

Reference [22] examines TAM, the theory of planned behavior (TPB), UTAUT2, and the Value-based Adoption Model (VAM). When these theoretical models, it was discovered that VAM behaved the best when it came to modeling user acceptance. The findings indicated that the public accepts extremely inventive items with little practical utility at large. In a similar manner, the research has demonstrated that the VAM has greater predictive power than other models [22], [23]. Because of this, the VAM model is the most accurate approach to determine the values associated with higher education institutions as a result of implementing the concept of the smart campus. Hence, the comparison between TAM, UTAUT, and VAM is presented in Table 1. Furthermore, Table 2 synthesized the existing studies that propose VAM to complement the weakness of TAM and UTAUT, respectively.

This aims to conceptualize an adoption model for smart campus and there is a general agreement upon the importance of privacy, security, and trust as significant factors for IoT

TABLE I
COMPARISON BETWEEN TAM, UTAUT, AND VAM

| Theory/ Model | Advantage | Disadvantage | Reference |
|---|---|---|---|
| TAM | Very simple and inexpensive with two generic variables (usefulness and ease of use). | The generic factors are insufficient for describing a complex situation because they do not consider users' existing associations with the system. | [26]–[29] |
| | The TAM model is straightforward and strong. | TAM excluded potential variables that may be significant. | |
| | Excellent for revealing attitudes toward the use of information technology. | Weak constructs and lack explanatory power and have inconsistencies amongst them. | |
| UTAUT | A model produced by combining eight existing models. | Additional external factors are still required for testing the adoption of various technologies in new contexts. | [26], [31], [32]. |
| | Places a greater emphasis on expectation performance. | Neglect to justify the users' expectations and beliefs that are likely to arise; does not place emphasis on personal expectation. | |
| | The model is best suited for use in the workplace. | Is not best suited for public settings. | |
| VAM | VAM behaved the best when it came to modeling user acceptance. | Still emerging and lack studies to justify its strength. | [22], [33], [34] |
| | Has greater predictive power than other models. | More studies are needed to verify the predictive power of VAM. | |

TABLE II
THE SUMMARY AND COMPARISON OF EXISTING STUDIES BASED ON VAM

| Authors | Perceived Usefulness | Perceived Enjoyment | Perceived Fee | Perceived Technicality | Perceived Value | Intention to Adopt | Perceived Privacy | Perceived Trust |
|---|---|---|---|---|---|---|---|---|
| Niknejad et al. (2019) | | ✓ | ✓ | | ✓ | | ✓ | ✓ |
| Sohn and Kwon (2020) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Pal et al. (2020) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |

deployment and acceptance [14]–[17], and the impact of these variables on IoT adoption and acceptance [35]–[37]. As a result, from the perspective of smart universities, empirical study concentrating on the impact of privacy, security, as well as trust was not conducted to answer these questions. Recently, the work by reference [38] has not addressed privacy and users' trust; however, the security and trust of IoT devices must be investigated in order to build public trust [38]. Studying these knowledge gaps could provide new insights on the full-scale use of IoT smart campuses by universities, particularly in developing countries. Hence, the success of IoT adoption in the future is thought to be dependent on the trust, security, and privacy of users. While the literature has shown the predictive power of VAM is higher than other models [22], [23]. Thus, this model is presumed to predict the values concerning higher educational institutions as a result of adopting the smart campus concept, as shown in Fig. 4.

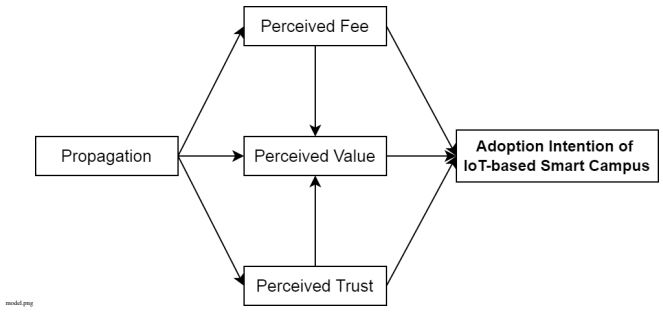



Fig. 4. The Smart Campus Adoption Model for Higher Learning Institutions

The propagation concept for the smart campus was conceived by [4]. Accordingly, the study insisted that the need for developing a generic model is still very important. The propagation was introduced in the early study with characteristics such as scalability, reliability, replication, security, privacy, and cost of deployment. The cost of deploying smart programs, termed as a perceived fee, should be straightforward to comprehend and quantify, which is presumed to predict adoption in this study as indicated by previous research [22], [23], [34]. Hence, the perceived fee is the unit cost that a consumer incurs by using IoT devices which covers purchasing, installing, and maintaining various smart campus devices. Moreover, perceived trust is an emotional condition and a vital component in technology adoption that helps users have confidence in a product or service and strengthen relationships [15]–[18]. This promotes users' trust in smart campuses or entities managing smart campuses based on the satisfactory behavior of the devices or the smart campus management entities.

The conceptual model intends to demonstrate the factors impacting the intention to adopt an IoT-based smart campus, which will help stakeholders and policymakers to see the value to be derived from the adoption of smart campuses to improve effective resource utilization, energy savings, informed decision, improved services, and risk mitigation. Specifically, the model will determine the impact of propagation of smart campus [4] on perceived fees [22], [23], [34], perceived trust [34], perceived value [22], [23], [34], and adoption intention of IoT-based smart campus solutions. The model shall also investigate the mediating role of perceived fees,

perceived trust, and perceived value on the adoption intention of smart campus solutions for full-scale use. Accordingly, the model shows a relationship between propagation and perceived fees, propagation and perceived trust, and propagation and perceived value. Moreover, the model shows that there is a relationship between perceived fees and adoption intention of IoT-based smart campuses, perceived trust and adoption intention of IoT-based smart campuses, and perceived value and adoption intention of IoT-based smart campuses.

## V. Conclusion

The purpose of this study is to serve as an introductory summary and a reference guide to smart campus, with a special emphasis on the adoption of these systems. It is discussed in the report that there is a significant adoption challenge that must be resolved in order to promote an IoT-based smart campus. The current study, in particular, emphasized that there are a variety of models in the technology acceptance literature that can be used to enhance technology adoption. According to the findings of this study, TAM and UTAUTs are the most prevalent models. However, recent research has focused on the value-based adoption model (VAM), which has been adapted to conceive the adoption model of smart campuses. This study evaluated the literature to discover commonalities among IoT adoption models that are suited for smart campus adoption and proposed a conceptual technology adoption model for smart campus adoption, which was the basis of this research.

### A. Limitations and Future Works

This study is not without some limitations. The conceptual study model needs to be validated. Therefore, future researchers may concentrate on validating and verifying the conceptual framework. Furthermore, the future study may use a scientific approach such as the hierarchical analytical process (AHP) to select the factors better to be considered for smart campus adoption. This technique has the capability to rank the factors in order to identify the most appropriate criteria to investigate the adoption of IoT-based smart campuses in higher education. The adoption model will aid in the promotion of the concept of smart campus, which is more environmentally friendly and contributes to the establishment of a more environmentally friendly campus.

## Acknowledgments

The authors would like to thank the Ministry of Higher Education and Universiti Putra Malaysia for using the Fundamental Research Grant Scheme (FRGS/1/2021/ICT01/UPM/02/2), which supported this work.

## References

[1] L. Hudson, A. Wolff, D. Gooch, J. Van Der Linden, G. Kortuem, M. Petre, R. ten Veen, and S. O'Connor-Gotra, "Supporting urban change: Using a mooc to facilitate attitudinal learning and participation in smart cities," *Computers & Education*, vol. 129, pp. 37–47, 2019.

[2] A. Caragliu, C. Del Bo, and P. Nijkamp, "Smart cities in europe. research memoranda series 0048 (vu university amsterdam, faculty of economics, business administration and econometrics)," *J. Urban Technol*, vol. 18, 2009.

[3] A. Arroub, B. Zahi, E. Sabir, and M. Sadik, "A literature review on smart cities: Paradigms, opportunities and open problems," in *2016 International conference on wireless networks and mobile communications (WINCOM)*. IEEE, 2016, pp. 180–186.

[4] N. Min-Allah and S. Alrashed, "Smart campus—a sketch," *Sustainable cities and society*, vol. 59, p. 102231, 2020.

[5] M. Musa, M. N. Ismail, and M. F. M. Fudzee, "A survey on smart campus implementation in malaysia," *JOIV: International Journal on Informatics Visualization*, vol. 5, no. 1, pp. 51–56, 2021.

[6] V. Ahmed, K. Abu Alnaaj, and S. Saboor, "An investigation into stakeholders' perception of smart campus criteria: the american university of sharjah as a case study," *Sustainability*, vol. 12, no. 12, p. 5187, 2020.

[7] M. Turner, B. Kitchenham, P. Brereton, S. Charters, and D. Budgen, "Does the technology acceptance model predict actual use? a systematic literature review," *Information and software technology*, vol. 52, no. 5, pp. 463–479, 2010.

[8] V. Venkatesh, "Adoption and use of ai tools: a research agenda grounded in utaut," *Annals of Operations Research*, vol. 308, no. 1, pp. 641–652, 2022.

[9] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The internet of things: Review and theoretical framework," *Expert Systems with Applications*, vol. 133, pp. 97–108, 2019.

[10] C.-L. Hsu and J. C.-C. Lin, "Exploring factors affecting the adoption of internet of things services," *Journal of Computer information systems*, vol. 58, no. 1, pp. 49–57, 2018.

[11] F. J. Riggins and S. F. Wamba, "Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics," in *2015 48th Hawaii International Conference on System Sciences*. IEEE, 2015, pp. 1531–1540.

[12] D. Lund, C. MacGillivray, V. Turner, and M. Morales, "Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand," *International Data Corporation (IDC), Tech. Rep*, vol. 1, no. 1, p. 9, 2014.

[13] C.-L. Hsu and J. C.-C. Lin, "An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives," *Computers in Human Behavior*, vol. 62, pp. 516–527, 2016.

[14] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[15] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[16] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad hoc networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[17] S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, "A security-and quality-aware system architecture for internet of things," *Information Systems Frontiers*, vol. 18, no. 4, pp. 665–677, 2016.

[18] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[19] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling trust dynamics in the internet of things," *Information Sciences*, vol. 396, pp. 72–82, 2017.

[20] J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1–14, 2017.

[21] D. Lin, C. Lee, and W. Tai, "Application of interpretive structural modelling for analyzing the factors of iot adoption on supply chains in the chinese agricultural industry," in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE, 2017, pp. 1347–1351.

[22] K. Sohn and O. Kwon, "Technology acceptance theories and factors influencing artificial intelligence-based intelligent products," *Telematics and Informatics*, vol. 47, p. 101324, 2020.

[23] D. Pal, C. Arpnikanondt, S. Funilkul, and W. Chutimaskul, "The adoption analysis of voice-based smart iot products," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10 852–10 867, 2020.

[24] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[25] U. A. Bukar, M. A. Jabar, F. Sidi, R. N. H. B. Nor, S. Abdullah, and M. Othman, "Crisis informatics in the context of social media crisis

communication: Theoretical models, taxonomy, and open issues," *IEEE Access*, vol. 8, pp. 185 842–185 869, 2020.
[26] R. El-Haddadeh, V. Weerakkody, M. Osmani, D. Thakker, and K. K. Kapoor, "Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement," *Government Information Quarterly*, vol. 36, no. 2, pp. 310–320, 2019.
[27] S.-c. Chan *et al.*, "Understanding internet banking adoption and use behavior: A hong kong perspective," *Journal of Global Information Management (JGIM)*, vol. 12, no. 3, pp. 21–43, 2004.
[28] J. Choi and S. Kim, "Is the smartwatch an it product or a fashion product? a study on factors affecting the intention to use smartwatches," *Computers in Human Behavior*, vol. 63, pp. 777–786, 2016.
[29] R. P. Bagozzi, "The legacy of the technology acceptance model and a proposal for a paradigm shift." *Journal of the association for information systems*, vol. 8, no. 4, p. 3, 2007.
[30] H. Sun and P. Zhang, "The role of moderating factors in user technology acceptance," *International journal of human-computer studies*, vol. 64, no. 2, pp. 53–78, 2006.
[31] V. Venkatesh, J. Y. Thong, and X. Xu, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology," *MIS quarterly*, pp. 157–178, 2012.
[32] P. Ajibade, "Technology acceptance model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches," *Library Philosophy & Practice*, vol. 1941, 2018.
[33] D. Pal, B. Papasratorn, W. Chutimaskul, and S. Funilkul, "Embracing the smart-home revolution in asia by the elderly: An end-user negative perception modeling," *IEEE Access*, vol. 7, pp. 38 535–38 549, 2019.
[34] N. Niknejad, I. Ghani, F. A. Ganjouei *et al.*, "A confirmatory factor analysis of the behavioral intention to use smart wellness wearables in malaysia," *Universal Access in the Information Society*, vol. 19, no. 3, pp. 633–653, 2020.
[35] G. F. Marias, J. Barros, M. Fiedler, A. Fischer, H. Hauff, R. Herkenhoener, A. Grillo, A. Lentini, L. Lima, C. Lorentzen *et al.*, "Security and privacy issues for the network of the future," *Security and Communication Networks*, vol. 5, no. 9, pp. 987–1005, 2012.
[36] D. Gessner, A. Olivereau, A. S. Segura, and A. Serbanati, "Trustworthy infrastructure services for a secure and privacy-respecting internet of things," in *2012 IEEE 11th international conference on trust, security and privacy in computing and communications*. IEEE, 2012, pp. 998–1003.
[37] S. Ransbotham, R. G. Fichman, R. Gopal, and A. Gupta, "Special section introduction—ubiquitous it and digital vulnerabilities," *Information Systems Research*, vol. 27, no. 4, pp. 834–847, 2016.
[38] S. R. Chohan and G. Hu, "Success factors influencing citizens' adoption of iot service orchestration for public value creation in smart government," *IEEE Access*, vol. 8, pp. 208 427–208 448, 2020.