Review

Revising Technology Adoption Factors for IoT-Based Smart Campuses: A Systematic Review

Radhwan Sneesl [1,2,*,†] **, Yusmadi Yah Jusoh** [1,*,†] **, Marzanah A. Jabar** [1,†] **and Salfarina Abdullah** [1,†]

1 Department of Software Engineering and Information System, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), Serdang 43400, Malaysia; marzanah@upm.edu.my (M.A.J.); salfarina@upm.edu.my (S.A.)

2 College of Science, University of Basrah, Basrah 61001, Iraq

* Correspondence: radhwan.sneesl@gmail.com (R.S.); yusmadi@upm.edu.my (Y.Y.J.)

† These authors contributed equally to this work.

Abstract: Smart education and the sustainable development of smart campuses have drawn significant research attention. This is enabled by intelligent devices that are widely attracting massive applicability in personal and big business contexts and can increase efficiency and convenience. This paper aims to present a solution to address the lack of a proper adoption model for smart campus initiatives. The evaluation and synthesis of the literature were conducted by following the systematic literature review (SLR) procedure. The study's findings revealed the taxonomy and IoT technologies leading to the wide adoption of IoT-based smart campuses. The technology adoption models and their corresponding variables help the authors identify and classify a suitable adoption framework for smart campuses. The limitations and challenges of adoption theories as they pertain to smart campuses are discussed. Finally, the study adapts perceived scalability, perceived replicability, perceived reliability, perceived privacy and security, perceived trust, the cost of deployment, usefulness, enjoyment, and technicality as adoption factors of sustainable smart campuses. This study offers practical and theoretical implications regarding the adoption and propagation of emerging smart campuses.

Keywords: smart campus; IoT; sustainability; adoption; SLR; factors

1. Introduction

Enterprise executives ranked the Internet of Things (IoT) as an essential technological advancement, surpassing artificial intelligence (AI) and robotics in importance [1]. The IoT is considered a significant development in information technology that can potentially increase convenience and efficiency in daily life. Hence, Hsu and Lin [2] believe that the IoT has the ability to integrate numerous technologies to improve overall quality of life. The number of IoT service users has widely increased, but little is understood about what motivates the continued use of such services [3]. According to [4], "smart terminology" is a buzzword that was initially coined to describe cell phones that dominate the market. An electronic device managed via smartphones is called a "smart device", and comprises music devices, smartwatches, smart locks, smart lights, smart washing machines, etc.

The IoT has had a profound and widespread impact on the world of information technology [5], and impacts everyone from individual users to large organizations. Similarly, the IoT is significant in the development of smart homes for private users and in the automation, logistics, manufacturing, commercial elements, and other business or educational perspectives of small and large educational institutions [5]. Hence, implementing IoT solutions across universities will undoubtedly benefit all individuals on and off campus. Furthermore, Min-Allah and Alrashed [4] reaffirmed that the implementation of the smart city concept could be realized at a different level of the environment (building, town, or region) and the IoT is an enabler of the sustainable smart environment. The growth of smart

cities and sustainable development has established a new standard for urbanization [6]. Accordingly, citizens of smart cities can benefit from a smart living environment, easy access to services, ubiquitous connectivity, intelligent decisions enabled by smart governance, and resource optimization. Similarly, smart cities can provide the highest quality services to improve healthcare, energy usage, transportation, and education [6,7].

Hence, the concept of smart cities can be extended to improve sustainable education infrastructure [7] with examples such as smart classrooms, smart payments, smart stadiums, and smart parking [8]. Universities have seen an explosion of several electronic devices used by students and on campus that are connected to the university network, resulting in a huge amount of data that could be used for decision making [9–11]. The promise of smart cities via the usage of smart technologies and IoT devices has pushed universities towards adopting the smart city concept on various campuses [4]. However, the notion of smart cities as well as smart campuses is still emerging. Despite their tremendous promises, security concerns continue to grow, such as data security, authentication, unauthorized access, and sustainability [6,7].

Nonetheless, the adoption of information technology enables universities to strengthen their economic sustainability and create a sustainable education system [12,13]. However, the success of this depends on the commitment of all stakeholders (government, industry, academia, and end-users) involved in the initiation, planning, and implementation [4,14–18]. Chuling et al. [15] identified three patterns pushing the realization of smart campuses: initiatives that are technology-driven, smart city-driven, and business process-driven. Recently, a knowledge management model for smart campuses [19], smart campus key performance indicators [20], a student management system for smart campuses based on 5G networks and the IoT [21], a mobile application for smart campuses [22], an IoT-based hybrid renewable energy system for smart campuses [23], a methodology proposal for smart campuses [24], and a roadmap to smart campuses based on the IoT were introduced [5]. Hence, there is a lack of an adoption model for smart campuses.

Nevertheless, there is a lack of common understanding concerning the concept of smart campuses in the literature [18,25]. A smart campus is a term used to describe digital technologies designed to optimize the maintenance and utilization of a campus' physical infrastructure to reduce overall energy consumption [4]. Moreover, the phrase "smart campus" refers to combining and implementing smart technology (IoT devices) with physical infrastructure to achieve significant service, decision, and sustainability improvements in educational institutions [4]. Thus, it is under the umbrella term "smart campus", which comprises a variety of solutions such as smart classrooms, smart grids, smart attendance via smart cards or facial recognition and student management, and infrastructure surveillance and monitoring [20,21,26,27]. Numerous towns and universities have implemented innovative solutions to enhance campus sustainability [4,20,28] in terms of energy conservation and security [28].

Accordingly, a generic model that can be used for smart campuses has not been established [4]. However, Omotayo et al. [29] applied a systems thinking analysis and further evaluated the systems thinking-SWOT analysis [30] to facilitate successful and sustainable smart campus transitions. Additionally, Ahmed et al. [8] investigated the stakeholders' perception of smart campus criteria, and Pandey et al. [5] proposed a new method of smart campuses which focuses on the IoT and explains the idea of smart campuses through the IoT. However, there is a lack of studies about the adoption of IoT-based smart campuses facilitated by technology adoption theories. Therefore, this study aims to review the current literature on the adoption of the IoT to help proliferate and provide insight concerning the adoption of the smart campus concept and ease the adoption process for the administration and decision-makers of higher educational institutions [11]. Thus, the objectives of this literature review include: identifying the taxonomy of the studies on IoT technologies and IoT applications leading to the smart campus concept; ascertaining technology adoption models and common variables suitable for studying the adoption of smart campuses; and classifying technology adoption factors of smart

campuses for full-scale use. Therefore, the following questions help the researchers address the objectives of the research:

- What is the taxonomy of IoT application areas or technologies leading to smart campuses or education?
- What are the technology adoption theories and common variables for IoT adoption that are suitable for the adoption of smart campuses?
- How are technology adoption factors for IoT-based smart campuses classified, and what are the criteria behind this classification?

Notably, this paper presents a solution to address the lack of a proper adoption model for smart campus initiatives. The paper is presented as follows: Section 2 presents the related literature review and motivation of the study. Section 3 describes the research methodology adopted to the selection of articles relevant for this review. Section 4 answers the research questions sequentially: the taxonomy of IoT application areas and technologies for smart campuses, technology adoption models and variables widely used in IoT adoption, and the classification of technology adoption factors. Section 5 discusses the open issues and challenges faced by IoT-based smart campus solutions and the rationale for smart campus adoption based on existing technology adoption theories. Moreover, this section also discusses a conceptual model for smart campus adoption. Finally, Section 6 offers concluding remarks.

2. Related Review and Motivation

The main focus of this work is to conduct a literature review concerning the theoretical framework for the adoption of technology as it relates to smart campus adoption and usage in order to promote the concept of smart campuses or smart education in the literature. Although there are few review papers in the literature concerning the concept of smart campuses, there is a limited number of papers concentrating on the technology adoption aspect of smart campuses. Table 1 summarizes the focus of various review papers on smart campuses.

Table 1. Summary of existing literature studies on smart campuses.

Related Work	Year	Focus
[31]	2018	A systematic review on smart learning which compares two databases and provides authors' details and the locations of their publications.
[32]	2019	Research on the current educational programs and issues in smart cities and a summary of several recent educational programs and issues.
[33]	2019	Investigates the role of the IoT in smart campuses and smart universities, highlighting IoT, cloud computing, big data, and artificial intelligence as the primary technologies used to implement smart campuses and smart universities. The authors emphasize the variety of devices that are used to support smart campuses, ranging from low-resource devices such as sensors to high-resource devices such as cell phones.
[4]	2020	Proposes a sketch of a smart campus based on smart city concepts. The authors also develop a list of smart campus initiatives that can be prioritized based on the university's needs and geographical location, using a variety of smart campus solutions.
[34]	2021	Summarizes existing directions focusing on education in the context of smart cities. The article focuses on the challenges and difficulties associated with education in smart cities.
[27]	2021	Discusses the surveillance system challenges and solutions of IoT-enabled smart campuses. The study covers five key dimensions including enabling technologies, physical infrastructure, system security, software analytics, and research methodology
[35]	2021	Focuses on smart campus implementation and initiatives in Malaysian universities, revealing that most institutions implement some aspect of smart campus initiatives such as smart management, smart learning, and green campus initiatives.

As presented in Table 1, the existing review or survey studies about smart campuses are deficient on the adoption issue of smart campuses. Precisely, Durán-Sánchez et al. [31] conducted a systematic review of smart learning, which reported the authors and locations of publications related to smart learning. The work by [32] provides an overview of current educational programs and issues in the smart cities research direction of several recent educational programs and issues in smart cities. Furthermore, the study conducted by Rico-Bautista et al. [33] is one of the early works that investigated the role of IoT in smart campuses and smart universities by highlighting the IoT as one of the primary technologies used to implement smart campuses and smart universities. Moreover, Min-Allah and Alrashed [4] reviewed the literature and proposed a sketch of a smart campus based on smart city concepts. The authors developed a list of smart campus initiatives based on the university's needs and geographical location. In addition, Molnar [34] covers education in the context of smart cities as well as challenges and difficulties associated with the concept. Furthermore, Anagnostopoulos et al. [27] reviewed the challenges and solutions of surveillance systems on IoT-enabled smart campuses, and [35] surveyed smart campus implementation and initiatives in Malaysian universities, covering smart management, smart learning, and green campus initiatives. Remarkably, none of the current studies address the adoption issue for smart campuses. Thus, this review study is distinguished from existing review papers by focusing on a different set of research questions with the intention of conceptualizing an IoT-based smart campus adoption model. Hence, the work focuses on leveraging the existing adoption models of IoT technologies to build an adoption model appropriate for smart campus solutions [9].

3. Method

A breakdown of the research methodology is presented in Figure 1. The stages were adapted to address the research questions formulated in the study. Specifically, after the motivation of the study was identified, the process of paper selection was conducted through a systematic review method, which specified the articles used for this study. The second phase was to determine the theoretical models used to adopt IoT in the literature, with their corresponding factors. The third stage involved filtering the factors to delete duplicates, which were used for the classification in the fourth stage. Additionally, the literature provided the researcher with a justification for conducting a systematic literature review (SLR), especially when it came to selecting the research studies for this review [36]. These include the fact that the SLR reviews are primarily focused on the challenge of obtaining empirical evidence, which is employed in information system research. SLR is a well-defined process that reduces the influence of literature bias and can provide information and evidence concerning consistent and inconsistent outcomes across a wide range of empirical methods [36,37]. The SLR process was conducted based on the recommendations identified from previous studies [37,38] and applied by many researchers [39–41]. The selection process of the research papers is presented in Figure 2.

Figure 1. Breakdown of the research methodology.

As demonstrated in Figure 2, the method of paper selection consisted of using three online databases to collect research articles regarding IoT smart campus adoption and usage. The inclusion and exclusion criteria of the papers are based on the recommendations by [32]. The selection methodology was conducted based on accompanying advances in the literature. This involved the utilization of the leading online databases to collect research papers (ScienceDirect, IEEE Xplore, and Springer) that are used for this review. We filtered the research papers according to qualification criteria such as publication period, the context

of the paper, and QoS assessment measurements. Finally, we conducted an evaluation of the eligibility criteria and carried out the final selection [42]. The selection methodology used and the context that was followed enabled the researchers to identify many research articles without having the issue of duplication. This can serve as a further guide for academic researchers on the importance of quality research articles. Similarly, the articles that did not satisfy the eligibility criteria were not considered for further assessment. These articles comprise book chapters or conference papers, white papers, surveyed papers, short papers, papers not in QoS performance metrics, non-English papers, and papers that do not cover technology adoption models or smart campus technologies. The usage of these criteria may contribute to the success of the adoption of smart campuses. A further breakdown of the search and selection process and the query used during the search process are presented in Figure 3.
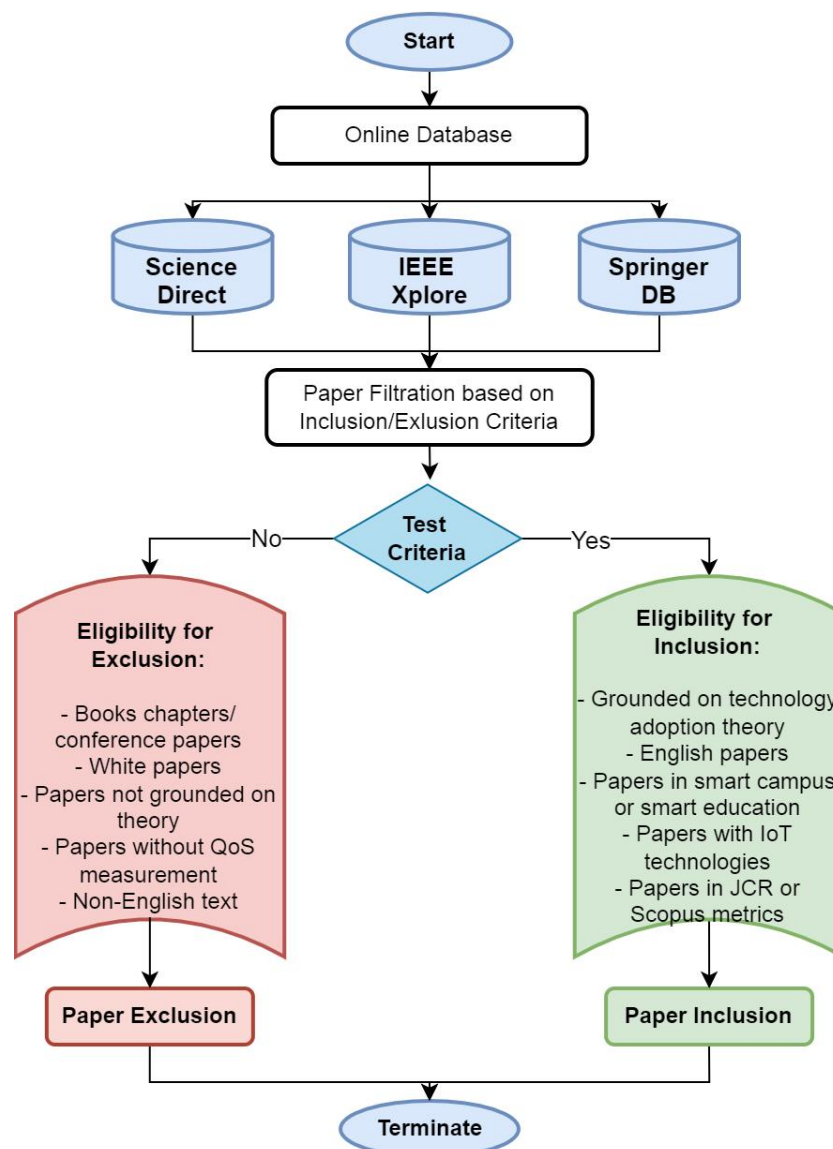

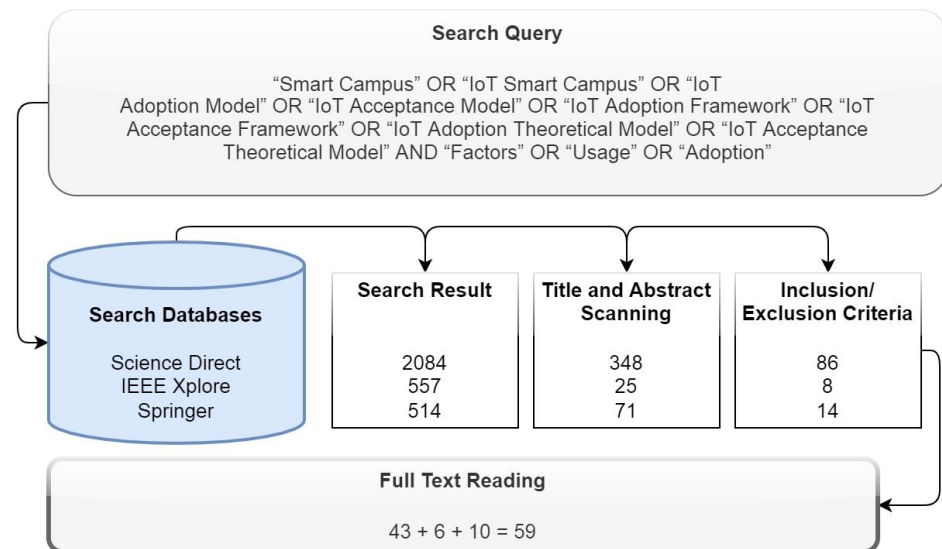**Figure 2.** Paper selection methodology.

Figure 3. Paper search and selection process.

4. Results

In order to conduct the literature review, this study follows the SLR guidelines that have been published in the literature [37,38,41]. As a result, the SLR is broken down into four steps, which are depicted in Figure 2 and, later, Figure 3. The SLR begins with a search for relevant articles, which is the first stage. Accordingly, a query is constructed based on keywords discovered in the literature and is used to search for published research, which is illustrated in Figure 3. The search results retrieved 2084 publications in ScienceDirect, 557 publications in IEEE Xplore, and 514 publications from Springer, according to the results of the search. Following that, the publications were screened based on the titles and abstracts that were scanned. During this stage, articles that were not connected to the research theme were not taken into consideration. Following this stage, additional inclusion and exclusion criteria were implemented to the publications that had been selected for further evaluation. Articles that are excluded from consideration include conference papers, non-English texts, and articles that are not open access. In contrast, articles that were considered are Index JCR or Scopus papers, as well as articles that have adopted or adapted technology acceptance theories in the research design. As a result, the final sample is composed of 108 articles that will be examined for full-text consideration. As indicated in Figure 3, a total of 59 publications were chosen as final study samples because they met all of the final eligibility criteria during full-text reading.

4.1. What Is the Taxonomy of IoT Application Areas or Technologies Leading to Smart Campuses or Smart Education?

This section focuses on the first research question: what is the taxonomy of previous studies in terms of IoT technologies and IoT applications? Hence, the evaluation of existing studies identified many IoT smart device applications, as shown in Figure 4. Specifically, some studies focus on adopting the IoT in a general application that does not consider any specific IoT devices [43–45]. However, location-based services have been investigated in [46], while smart cities with autonomous vehicle (AV) acceptance were evaluated in [47], and the adoption of smart cities for public services was investigated by [48]. Furthermore, the investigation of NFC and RFID was reported in the literature concerning their adoption in industry logistics and supply chain management [49–51]. The study concerning the adoption of smart farming technologies (SFTs) in agriculture and agricultural supply chains was also identified in the literature [52–55]. The use of a wireless sensor network (WSN) was investigated by [56]. Moreover, the adoption of smartwatch wearables [57–60] and IoT wearable fitness trackers for healthcare/fitness [61], smartphone [62], voice assistants (VAs) [63], and smart TV terminals [64] was studied by various researches. Moreover,

studies encouraging the adoption of IoT-enabled smart homes and services were revealed during the review [65–68].
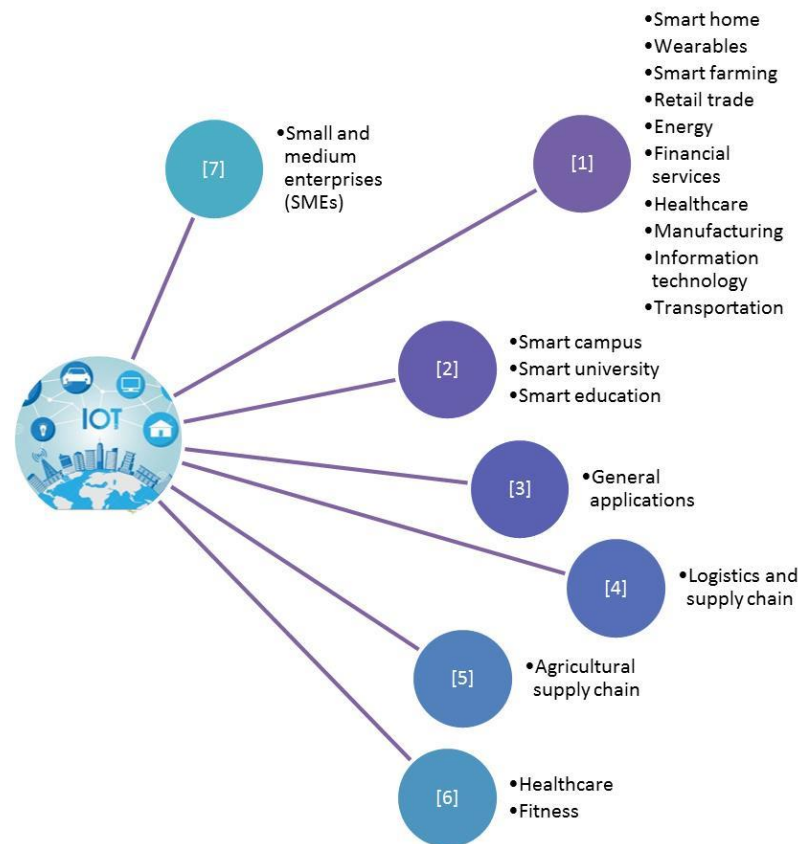

Figure 4. Taxonomy of IoT applications areas: [1] Nord et al. (2019); [2] Min-Allah and Alrashed (2020), Muhamad et al. (2017); [3] AlHogail (2018), De Boer et al. (2019); [4] Caffaro et al. (2020); [5] Jayashankar et al. (2018), Yamin and Alyoubi (2020); [6] Kao et al. (2019); Kim et al. (2016); [7] Won and Park (2020).

Furthermore, smart healthcare devices such as glucose monitoring systems (GCMS) and electronic medical records (EMR) to support healthcare service delivery for IoT-based healthcare have been recognized in the literature [60,69–71]. Additionally, many IoT technologies have been identified from existing studies concerning technology acceptance theories. The user adoption of EMR/IoT-based home energy services was examined by [72,73]. Moreover, the propagation of smart factories via small–medium enterprises (SMEs) was reported in previous studies [74,75]. The studies concerning the adoption of other IoT technologies such as AI-based intelligent products [76], IoT-based smart meters [77], IoT service orchestration [78], mobile cloud services [67], and cloud computing [79] were investigated.

Equally, the IoT technologies investigated by various studies were used to solve a particular problem in a specific area of application. Several areas of application were identified in the literature. Hence, Figure 4 presents the IoT application areas that were uncovered by the literature evaluation, analysis, and synthesis.

Smart Campus Concept and Technologies

The literature regarding smart explanations differs, but the focus is on how smart technologies leverage education services. A smart campus is viewed as an integration of computing technologies in the cloud and IoT devices that assist the university's management, teaching, and research activities [4,9–11,80]. Nevertheless, work by [14] has categorized IoT-based solutions into two classifications that reflect smart education concepts, namely, smart universities and smart campuses. Thus, the authors highlighted that

the concept of smart universities concentrates on the applications that will improve the universities' infrastructure and administration of academic services. The smart campus concept is used for external entities with financial and economic perspectives. However, several works have suggested that smart campuses and smart universities are used interchangeably, with the concept of smart campuses appearing to be more popular [15,81] as cited in [4].

However, the concept of smart campuses is still emerging [82], and this concept refers to smart education that allows the application of emergent smart technologies that collaborate with advanced educational practices, techniques, and tools [83] for the effective delivery of learning services [84]. The concept of the smart campus is derived from smart cities. Min-Allah and Alrashed [4] insist that a smart campus should share many things with a smart city since the university campus is similar to a small-scale city. Thus, smart cities aim to improve the quality of people's lives through technology. Education is found to be one of the entities of smart cities. Therefore, smart education terminology is a term that describes education delivered by smart cities [34]. Some of the major entities of smart campuses and smart education derived from the concept of smart cities are depicted in Figure 5. The smart campus concept was based on several works in the literature [4,34,85].
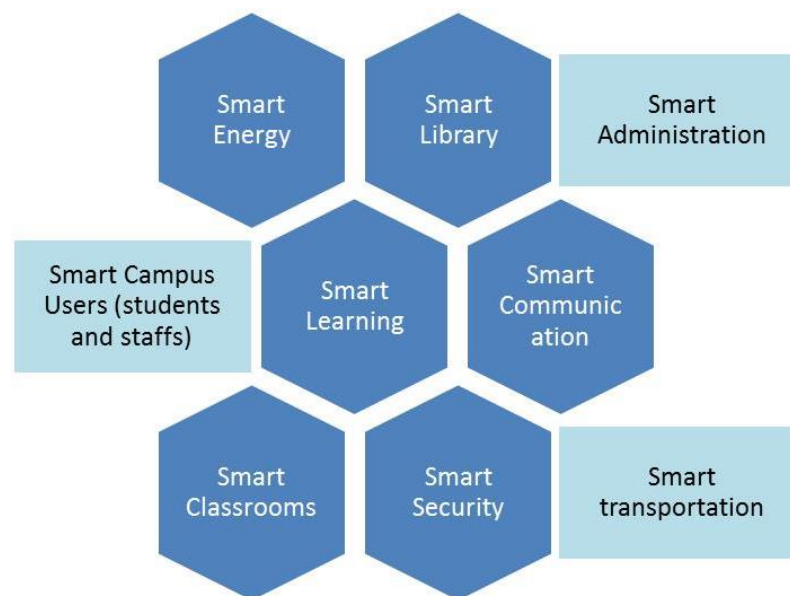

Figure 5. Major entities of a smart campus based on the smart city concept [4,34,85].

Various technological advancements have pushed for the realization of smart cities and smart campuses. For example, Kiryakova et al. [83] reported the penetration of technological advancements such as social media and internet-enabled resources into society, making citizens rely on technological resources to achieve their daily activities. As a result, citizens share more connections and effectively engage in the digital space to carry out their daily activities. Thus, the data generated by smart education approaches are, to a large extent, generated from the actions of students, teachers, and employers online [82]. Similarly, many solutions have embraced operating based on the data and information generated by IoT and other smart devices regarding smart campuses. A few examples of such solutions include the central intelligence layer introduced to provide services at the application level [86], services which comprise socializing, sharing events, mobility, and signaling problems [87]. The solutions are classified into three domains: practical life, social life, and academic life [88].

Moreover, many contactless technologies that are better than keyboards are used to provide an easy method to access buildings or equipment. In addition, IoT supports the real-time monitoring and reporting of environmental status. The transition in education has made IoT a mandatory course for all engineering students [89]. The concept of cloud com-

puting is also adopted to manage various information effectively and efficiently and provide real-time data services [16,79,90]. iCampus is a popular model considered for smart campuses that maps technological applications implemented in smart campuses [18]. Figure 6 summarizes the technology solutions supporting smart campuses identified through this investigation based on empirical research, as well as technologies for future research. These taxonomies of the technologies were derived from our investigation of the existing studies.
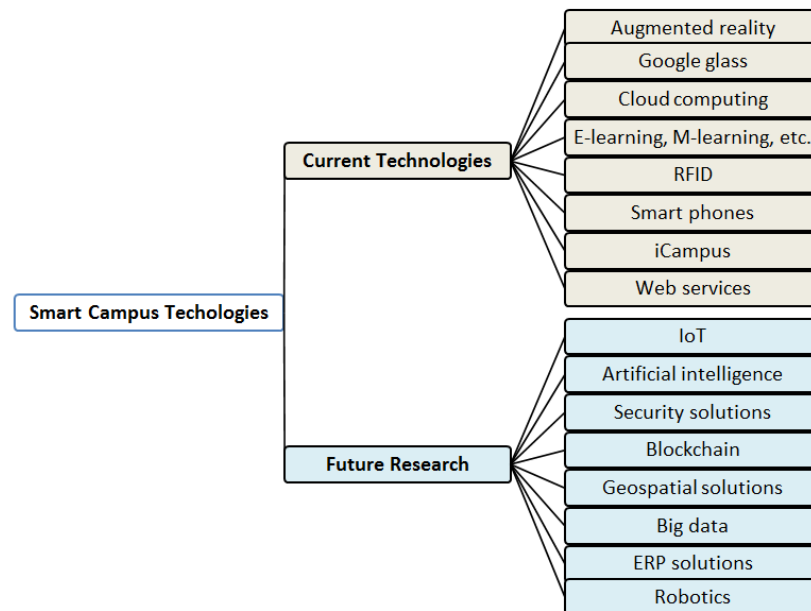

Figure 6. Technologies supporting smart campuses [16,18,79,85,90–98].

The technology in augmented reality (AR) can provide a video-based interface to support training and provide different experiences for trainers [91,92,99,100]. The work by [91] investigated whether AR-based online wearable guides improve learners' situational awareness, while [92] studied the adoption of AR in training. Google Glass is another smart technology used in educational institutions to support teachers and learners [93]. Moreover, Ashwin and Guddeti [101] introduced an automatic inquiry-based instruction system as a teaching strategy. The system was tested and evaluated in four different learning environments: e-learning, classroom, flipped classroom, and webinar environments. Mobile learning (M-learning) is also considered a new approach for learning, helping students access learning resources and easily conducting educational tasks [94]. M-learning avoids spatial or temporal restrictions by using model devices that are considered robust devices that support smart, easy and flexible learning.

Several studies have considered the smart campus to be a promising trend that was discovered as a result of digital campus development [15,16,18,90] through the usage of suitable technologies and the provision of internet services [102]. These technologies comprise the usage of various IoT service solutions [103] and cloud computing to integrate isolated systems [16,79,90]. The IoT services are created by transforming common solutions and objects within the educational institution's environment as intelligent solutions or objects through sensors [104,105]. The transformation of a common object into a comprehensive intelligence device is for supporting intelligent decision-making within the campus environment [106]. A smart campus supports the learning cycle within and across the campus ecosystem and aids the development of services and applications effectively [107]. Additionally, this increases the performance of the campus and improves student graduation quality [102]. The realization of the smart concept simplifies the three aspects of campuses, namely, teaching, management, and the service of the campus stakeholders [15,18].

Big data plays a significant role in smart cities; this role can also be provided to the smart campus model. Thus, the big data for smart campuses can significantly transform every area in the educational institution's economy as it does in the city through smart cities [108]. The transformation can enable universities to actualize the requirements and learning principles of smart city applications by identifying the key characteristics and features of a smart environment. The features and characteristics could comprise sustainability, improved quality of life, governance, resilience, and the intelligent management of resources and facilities [97,98]. Additionally, the application of artificial intelligence (AI) through machine learning (ML) and deep learning (DL) was encouraged to provide the smart campus with the capability to optimize the usage of resources and facilities [85]. Moreover, Sinha et al. [96] supported these claims by investigating the acceptance of robotics in the workplace [96], a typical example of a programmable machine learning system.

Additionally, the study conducted by Tavana et al. [95] unveiled the application of enterprise resource planning (ERP) systems that use the IoT to collect and transfer data between individuals and databases stored in the cloud and managed by ERP solutions. Moreover, cloud computing provides the efficient storage and processing of data; AI provides intelligence processing; big data manages a large volume of real-time data collected from IoT devices; IoT ensures the communication of the network of devices; blockchain handles trusted transactions and agreements; and security solutions provide mechanisms and protocols to secure IoT devices and systems. In addition, data visualization and IoT were exploited for increasing the sustainability and safety of smart campuses [28]. Figure 6 shows technology solutions supporting smart campuses for future research. This taxonomy of the technologies is derived from existing studies.

4.2. What Are the Technology Adoption Theories and Common Variables for IoT Adoption That Are Suitable for Smart Campus Adoption?

This section focuses on addressing the second research question concerning the existing theories and common variables studied in previous research. To address this question, the present study recognizes that the papers downloaded for this study based on the eligibility criteria do not provide enough papers on technology adoption for a smart campus to answer this research question. Nevertheless, the present study identified and selected 31/59 papers based on technology adoption theories for IoT devices across various application areas, and 28/59 papers are based on technologies supporting smart campuses. Thus, Table A1 (Appendix A) presents a summary of various constructs corresponding to the theoretical model found during the synthesis of the literature. Additionally, the frequency and popularity of theoretical models can be observed in this section. Hence, the analysis of the existing research concerning the adoption of IoT technologies or smart devices via technology acceptance theories has shown that the technology acceptance model (TAM) is the most popular theory tested in this context. The generic constructs of TAM include the perceived ease of use (PEoU) and perceived usefulness (PU). Several other studies have introduced and tested new constructs to improve the weakness associated with the TAM theory (Appendix A; Table A1).

Similarly, several other theories exist in the technology acceptance literature. Some of these theories include the unified theory of acceptance and use of technology (UTAUT) and UTAUT2, the theory of planned behavior (TPB), the value-based adoption model (VAM), and the theory of reasoned action (TRA). Table A1 (Appendix A) presents the list of the theoretical models and their corresponding constructs (i.e., whether they are generic or improvement constructs). The findings also reveal integrated models, a relational structure/hierarchical map, an ordered logistics model, and a trust framework. Most of the constructs and variables found in these models were presented in the models reported in Table A1 (Appendix A). The researchers observed that most of the research conducted based on an integrated model was linked to the most popular technology adoption theories.

The Popularity of Technology Adoption Models

According to [82], there is a rapid increase in academic research concerning smart education. However, the existing studies do not show the new artifact design of the smart campus. This would provide insight and knowledge to help the progress of smart campuses and address the aspirations of educational institutions. Moreover, the study conducted by Adamkó and Kollár [86] is one of the popular works that discuss the concept of smart campuses more broadly, specifically focusing on improving some of its aspects. However, Min-Allah and Alrashed [4] insisted that the need for developing a generic model is still very important. Thus, this study was conducted to close this gap by introducing a technology adoption model based on existing literature to guide the developers and policymakers of smart campuses' technological resources and design new smart education solutions that will be easily integrated and accepted by the users of educational institutions. Therefore, the technology adoption framework can be viewed as a conceptual solution model that would support students' and staff's adoption of smart campus solutions to improve learning and career development for a better future.

The literature analysis has revealed that TAM is the most studied theory for the adoption of IoT. However, the strength and limitations of the theoretical models used for technology acceptance theories are available in the literature, although the literature concerning IoT adoption is still emerging.

However, according to [48], there is much criticism regarding technology adoption models such as TAM since they do not take into account behavioral intention derived from complicated relationships involving earlier use perceptions and other factors. The work by [109] insists that the general factors of TAM (usefulness and ease of use) are insufficient for describing a complicated situation since the variables do not take into account users' existing relationships. The TAM model is straightforward and ineffective, as it does not include any potential variables that could be relevant [57]. The assumption about the relationship between intention and actual behavior has been questioned in many pieces of literature since it cannot ensure actual use [57]. The authors of [110] also assert that the TAM constructs have a weakness because of a lack of explanatory capacity and contradictions that exist between them. Additionally, the UTAUT theory highlights distinct technologies while failing to adequately justify the users' expectations and beliefs that are likely to arise while utilizing the technology [111].

Furthermore, UTAUT places a greater emphasis on expectation performance than it does on personal expectation. As a result, the UTAUT model is more appropriate for workplace situations than it is for public adoption. Despite this, numerous studies contribute to the prediction of intention and behavior based on the UTAUT model [48]. Figure 7 demonstrates the popularity of the adoption models.
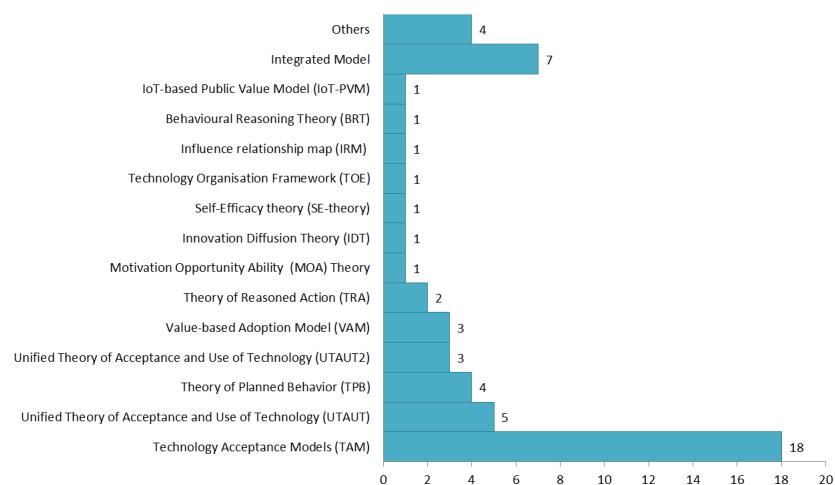

Figure 7. Frequency of technology adoption theoretical models.

4.3. How Are Technology Adoption Factors for IoT-Based Smart Campus Adoption Classified, and What Are the Criteria behind This Classification?

The taxonomy of the technology adoption factors is created based on the several studies that conducted a hierarchical analytical process (AHP) or have previously classified the factors. This could be based on some criteria by the previous researchers. Specifically, one of the used criteria is the technology–organization–environmental (TOE) framework. For example, Sharma et al. [112] classified the technology, organization, environment, and economic factors. The relative advantage, compatibility, complexity, security, and the quality of service are categorized under technology. The organizational category includes readiness, resistance to change, organization size, and top management support, most of which were not found in this study, except for innovativeness from the users' perspectives.

Furthermore, the environmental and economic factors cover pressure (competitive and partner) and cost (transaction, service, or losses). Secondly, Lanzini et al. [113] classified the factors into technology, organization, and environment. Similarly, the technological factors cover cost, governance, results observability, perceived compatibility, perceived ease of use, perceived usefulness, privacy, security, and trialability, among which only governance was not found in our study. Additionally, the organizational category covers people readiness, process readiness, technology readiness, top management enthusiasm, top management expertise, and top management support and the environmental factors include customer influence, competitive pressure, cooperation with ICT providers, environmental impact, government support, regulatory status, reputation, and trading partners. The classification in reference [114] was broken down into technology, organization, environment, security, perceived usefulness, and ease of use. Similarly, the technological category includes reliability, complexity, compatibility, and availability; the organizational category includes cooperated strategy, management support, technology competence, cost effectiveness, and budget availability; the environmental category includes regulation, the convenience of use, pressure from external factors, and consumer expectations; the security category includes authentication, authorization, integrity, confidentiality, non-repudiation, and privacy; the perceived usefulness category includes sharing, medical history, time sharing, error identification, and quality care; and, finally, the perceived ease of use category covers usability, customization, accessibility, responsiveness and user interface. Lastly, the classification of Pal et al. [66] covers service-specific characteristics (usefulness, innovativeness, perceived reliability, interoperability, service cost), end-user-specific characteristics (privacy concerns, psychological barriers, self-efficacy), and environmental characteristics (home administrative policies, government policies).

The Classification of the Factors

The factors identified in the literature were collated. Remarkably, this study identified many factors (112) classified based on the knowledge acquired from previous studies and thematic analyses [66]. Firstly, duplicate filtering revealed 77 factors. Then, the second duplicate filtering was applied through thematic analysis, which resulted in 52 factors, as presented Figure 8. While analyzing the factors obtained from the articles studied through systematic review, we tried categorizing the technology adoption factors into certain themes [66,112–114]. Four broad themes are recognized as: (a) technology-specific factors, (b) organizational-specific factors, (c) environmental-specific factors, and (d) end-user-specific factors. Figure 8 presents the broad themes and their corresponding factors. Hence, 52 reasonable technology adoption factors are finally classified accordingly.

During the thematic analysis, this study did not identify the complexity factor; it was discovered and classified as a technological component in previous research that applied AHP [112,114]. Moreover, prior studies have classified and merged factors according to their contextual meaning. For example, perceived usefulness, performance expectancy, effectiveness, personal and societal benefits, and perceived benefits are conceptually similar; they are considered a single factor (usefulness), rather than five. As a result, perceived usefulness and performance expectancy were combined into a single factor. Similarly,

perceived ease of use, effort expectancy, perceived technicality, usage barrier, and perceived behavioral control shared conceptual commonalities. Therefore, they are treated as a single component (ease of use) rather than five. Since all five factors were associated with problems in usage, they were merged into a single factor [63,76]. In addition, Kao et al. [61] adopted the technological awareness notion of domain-specific knowledge [115]. Accordingly, technological awareness refers to users' knowledge and comprehension of a certain technology or product [116]. Numerous studies have established the importance of perceived enjoyment (similar to hedonic motivation) in examining individuals' intrinsic motivations for adopting and using commercial products [59,73].

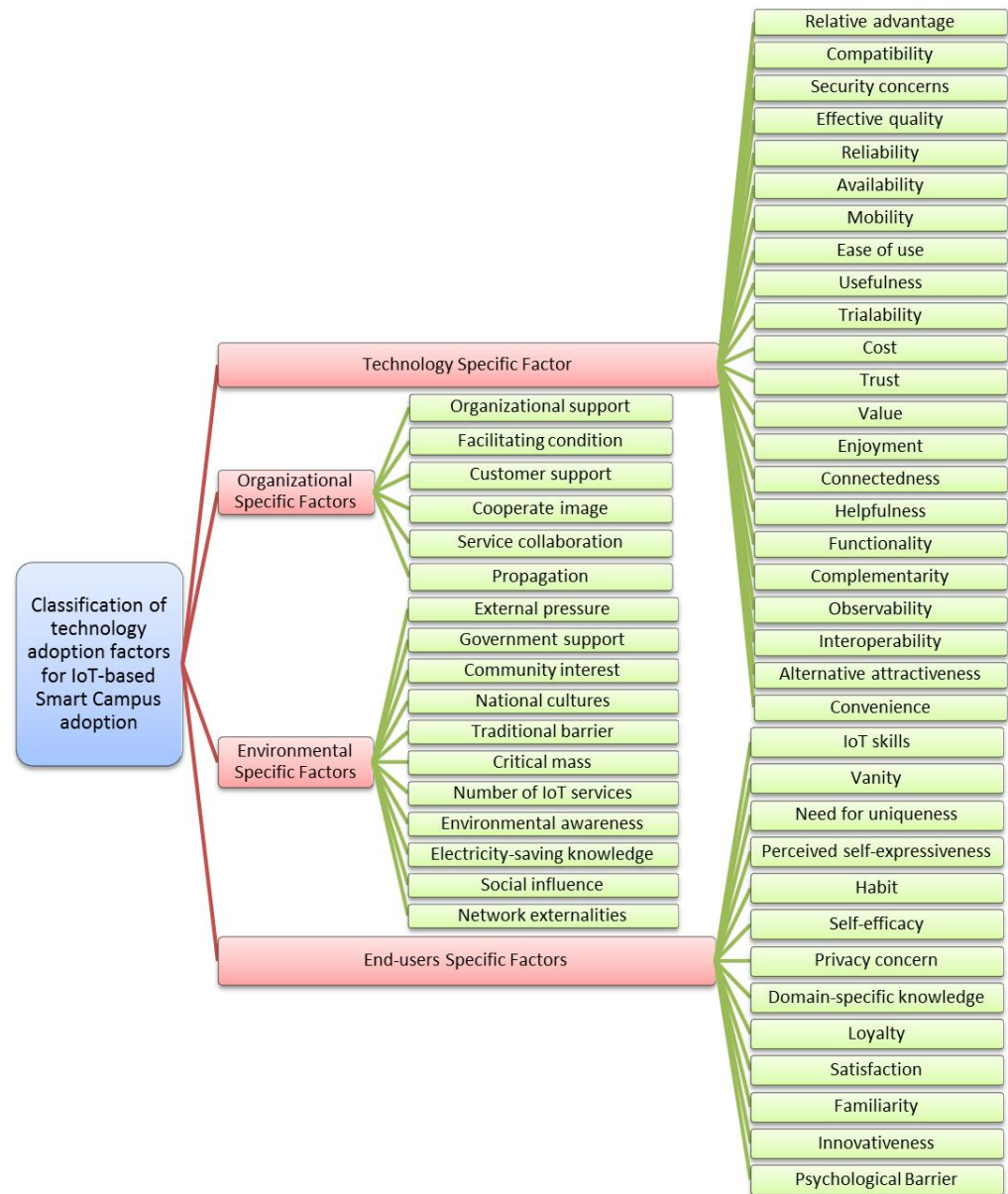**Figure 8.** Classification of technology adoption factors for IoT smart campuses.

5. Discussion

This section discusses the open issues and challenges of smart campus adoption, motivations for future research, and the adoption of smart campuses.

5.1. Open Issues and Challenges of Smart Campuses

According to [4], a smart campus adheres to smart cities' challenges and issues. Technology drivers and smart cities are influencers of smart campuses [15]. IoT solutions are entities driving smart cities through IoT-based smart devices. Thus, this study identifies and reveals some unresolved problems and challenges facing the concept of the smart campus. The most important are system security, identity management, access control, and trust in IoT smart products and services [27]. Insecure authentication methods create a trust gap across IoT network gateways [25,117] that may be part of a smart campus system, exposing these devices and their data to criminals. Another issue is the use of centralized, conventional IT computing systems and network models in a smart campus ecosystem that is decentralized and self-governing. The IoT smart devices themselves are still emerging, and any entity that has a part to play in the smart campus must adapt to the demands of this new ecosystem. The complexity, scalability, and management of the environment are all open issues in these systems that include an ever-increasing number of devices and applications.

The IoT network's complexity issue from the various types of devices that link to the edge, fog, and cloud could affect the success of a smart campus. Furthermore, the constantly changing attacks and threats lurking in IoT systems and services and the sheer number of factors that lead to security breaches are outstanding issues due to this heterogeneous existence. As a result, the network's scalability is undoubtedly a significant concern [117]. Furthermore, even though IoT is a decentralized environment, system management is not always considered, particularly when it comes to credential and certificate distribution and revocation, and transactional traffic is often mixed with administrative data movement. Similarly, security is considered a central aspect of any model. Other security challenges may include data confidentiality, device management, the integrity of cyber-physical systems, pivotal device pairing [118], and information security [119]. Moreover, the rapid adoption of smart cities has created concerns about data security, authentication, unauthorized access, device vulnerability, and sustainability [6,7]. As a result, as explained in the paper, generic and effective security solutions should be used in the design stage to mitigate risks and vulnerabilities.

The nature of IoT deployment and cloud computing for smart campuses, which raises issues about privacy, security, and trust, is a source of concern [120–122]. Security and privacy have been identified as the most significant impediments to the growth of the IoT and cloud computing [121,122]. Furthermore, privacy and security issues have an impact on the intention of IoT adoption, as evidenced by [43]. In accordance with the findings of [123], the issue of trust is considered difficult. Despite the fact that trust does not have a precise definition, it is widely recognized as being crucial in the field of information systems literature [124]. The concept of trust is closely associated with the concepts of reputation and dependability [125]. Trust in the relationship between entities (users) and trust in the system from the perspective of the users are two aspects of trust [126]. When it comes to adopting and using IoT technologies, trust is essential [1]. According to the framework developed by [127], trust should be considered throughout the entire IoT development process. A further contribution was made by [128], which presented trust computation models and provided recommendations for trust computation research. Figure 9 depicts the IoT security challenges as concerns for the success of smart campuses.

The complexity of a decentralized IoT environment has made the system independent from enforcing proper security solutions from a single party; rather, it is the responsibility of all actors concerned, from suppliers to producers, policymakers, developers, and the end-users. Although, it is possible to mitigate the risks associated with security breaches if the security issues are identified early in the product planning and design process and if certain simple mitigation measures are in place. Enactment and standardization would make production and development processes easier, provide a business catalyst for mass adoption, and improve the protection of IoT products and services. However, security will have to be built in for IoT and smart campus devices to stand a chance against

the challenges that technological advances will bring [25]. With advances in quantum computing, artificial intelligence, and cognitive systems and the continued growth and widespread acceptance of the IoT ecosystem, existing security practices and methodologies will become obsolete [117].

Figure 9. Smart campus IoT security challenges [1,43,120,121,123–127].

Moreover, Miloslavskaya and Tolstoy [129] present four classifications for data circulating in smart devices from an information systems perspective: data collected from smart devices, applications, and other sources; data in IoT data streams (network traffic or network packets); data segregated by IoT users; and data locked up in disparate security devices, applications, and databases. The storage of each of these types of data generates enormous amounts of data in various formats, for various purposes, and frequently with a variety of different information systems policies and even compliance requirements. One issue is figuring out how to structure, consolidate, and visually present all of these types of storage in a way that enables smart campus information systems management to make timely and informed decisions. Furthermore, the smart campus can address specific issues and improve the overall quality of education and student and staff life. Similarly, Ande et al. [130] emphasized that one of the most significant global challenges we face today is reducing energy consumption. Energy has developed into a critical human commodity.

5.2. Motivation for IoT-Based Smart Campus Adoption

This review aims to identify a technology adoption model suitable for promoting the concept of smart campus adoption for future studies. Thus, present studies concerning IoT adoption were reviewed to identify the existing studies' weaknesses. Accordingly, the findings revealed that there is a consensus regarding research methodology and additional validation procedures to validate new models [54]. Reference [74] emphasized that weak research design and analysis methods will not reveal a strong relationship between the variables. Some studies lack an investigation of a specific application of IoT devices [44,45]. Hence, there is a strong need for theoretical extension in the context of IoT-specific devices [50]. Similarly, having a small sample size is among the weaknesses of the research designs of existing studies, preventing them from providing a significant

result [51,59,69,74]. One key benefit of the literature review is linking present studies with previous work based on existing theory.

Moreover, the dependent variable in the study of [57] is not the actual adoption but the intention to adopt. Similarly, Alraja et al. [71] do not investigate actual use behavior for healthcare services. Additionally, Park et al. [67] draw further variables related to wireless services exposed to the risk of a security breach. The five risk factors presented in [67] require an additional analysis of the causality effects. Many predictors of the adoption of the IoT such as culture, lifestyle, social influences, personality, and cost were lacking from the literature. Logistics information platforms from the enterprise perspective is another area requiring future research [43]. The study of [64] does not consider users' characteristics such as smartphones or IT service habits and their capacity for personal innovation. Moreover, Han et al. [49] insist that factors such as technology readiness and facilitating conditions that can affect the use of NFC by other visitors to improve their understanding of NFC use limited their study concerning NFC adoption. However, facilitating conditions are one of the key constructs in the UTAUT model and were tested by many studies showing significant results. However, the perceived enjoyment and usefulness were not significant, according to the study by [67]. Hence, the hedonic motivation or perceived enjoyment and price value are among the extensions of UTAUT found in UTAUT2, which are overlooked by existing studies [52,65,69]. The coping behaviors that were employed as an ultimate consequence in the study of [46] were examples of perceptual decision making rather than actual behavior. The model proposed by [47] is based on the current perceptions of Millennials. Perceived concerns and mobility-related efficiencies were not addressed. This could offer new insight into IoT adoption and usage.

The analysis unit focused on cross-cultural perspectives rather than citizens' perspectives and behavior towards IoT use in public sector services [48]. Behavioral constructs that can explain patients' behavioral and psychological traits in the time of pandemics are not covered [70]. The work by [72] is limited to risk perception and overlooks other variables. The influence of the correlation and control variables between the independent variables was not analyzed as reported previously [75]. Furthermore, the work of Chohan and Hu [78] does not address privacy and user trust; however, IoT devices' security and trustworthiness need to be studied to increase public trust. Similarly, individual characteristics and empirical tests thereof, which can be associated with the intention to use information-oriented services, are lacking in a study conducted by [68]. Recently, Pal et al. [63] encouraged wider demographics comprising individuals, households, and business environments to help understand the adoption factors. Additionally, the perceived value was not considered by [71].

Furthermore, the work by [59] could be extended to smart technologies, such as smart medical devices. Moreover, other factors that are identified as limitations of existing studies include risk-taking behavior, innovation, cultural factors, and demographic factors [45,60], as well as the dynamics of users' behaviors toward IoT-based wearable fitness trackers [61]. Additionally, perceptions of value, risk, and even value-in-use evolve across various phases of IoT adoption, and need to be addressed [55]. A moderation effect was lacking from existing studies [53,58]. Expressly, the studies of Yamin and Alyoubi [56] are limited due to a lack of addressing mediating and moderating causal relationships among task technology factors. In addition, Alkawsi et al. [77] omitted the UTAUT2 moderators of experience, gender, and age. Moreover, a lack of a widely accepted research technique that connects existing ideas, frameworks, or models is a barrier to robust validation [54]. The majority of the study has not been applied to university settings in order to promote the concept of smart universities or smart campuses.

5.3. Adoption Model of IoT-Based Smart Campuses

This study aims to review IoT technology adoption models in order to conceptualize an adoption model appropriate for the adoption of smart campus solutions [9]. Hence, the literature review has identified a dearth of research on the adoption of IoT-based

smart campuses as supported by technology adoption theories. Moreover, there is a lack of previous reviews and surveys on smart campuses that comprehensively address the adoption issue [4,27,32–35]. Surprisingly, very few of the current studies address the topic of smart campus adoption [8], which focuses on stakeholders' perception criteria of smart campuses. As a result, the effort focuses on IoT technology adoption to develop an adoption model tailored to smart campuses. Therefore, the conceptualization of the smart campus adoption model is discussed as follows.

Firstly, the knowledge obtained through the literature analysis has shown that technology adoption studies are classified into four primary classifications. As previously reported, four broad themes are recognized as (a) technology-specific factors, (b) organizational-specific factors, (c) environmental-specific factors, and (d) end-users-specific factors. The technology-specific factors cover the technological features that are significant to the users. The organizational-specific factors relate to the organization's characteristics and resources (higher institutions), including the size, the degree of centralization, the degree of formalization, managerial structure, human resources, the amount of slack resources, and the linkages among employees. The environmental-specific factors encompass the size and structure of the institutions, their competitors, the macroeconomic background, and the regulatory environment such as government policies. Finally, the end-user-specific factors entail the personal characteristics of the users [131,132]. Hence, Figure 10 represents how the classified technology adoption factors affect the adoption intention of IoT-based smart campuses.
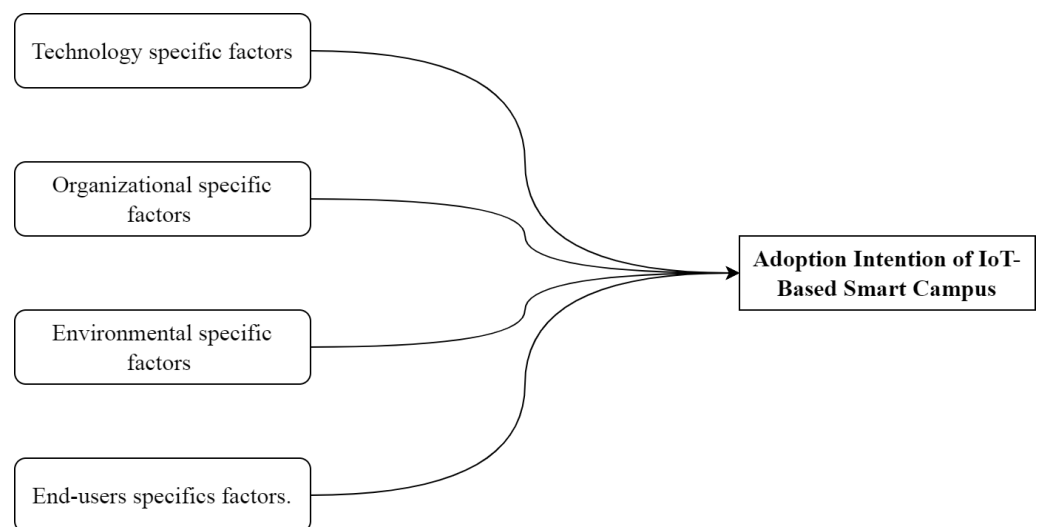

Figure 10. Adoption intention of IoT-based smart campuses.

Secondly, according to the literature review, current research has compared TAM, TPB, UTAUT2, and the value-based adoption model (VAM) [63,76], and it was discovered that VAM performed the best when it came to modeling user acceptance. The findings of these studies demonstrate that consumers are willing to tolerate extremely innovative products that have little practical usefulness. The literature has also demonstrated that the VAM has greater predictive power than other models [63,76]. As a result, the VAM model is the most accurate in predicting the values associated with higher education institutions as a result of the adoption of the smart campus idea. Hence, the adoption model intends to demonstrate the impact of smart campuses to help stakeholders and policymakers see the value derived from the adoption of smart campuses to improve effective resource utilization, energy savings, informed decision making, improved services, and risk mitigation [10,80,133,134]. Therefore, the conceptual model adopted the generic VAM constructs (usefulness, enjoyment, technicality, and cost), trust, and privacy and security as factors influencing the intention to adopt IoT-based smart campuses, as shown in Figure 11.
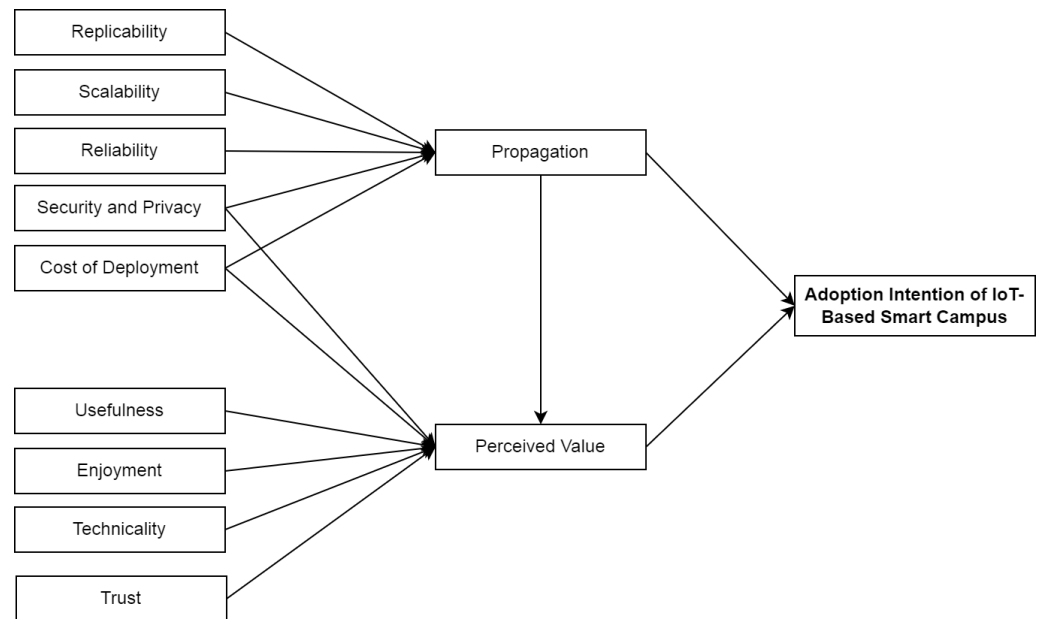
Figure 11. Conceptual model for IoT smart campus adoption.

Therefore, the VAM's usefulness, which is similar to the perceived usefulness of TAM, has been empirically tested to predict the behavioral intention or adoption of new technology [43,44,47,48,50–53,57–59,63–65,67,70,73,75–78,111,135,136]. Hence, the usefulness is the degree to which an individual believes that using the IoT or smart device will help them to attain gains in job performance. Similarly, the enjoyment was regarded as hedonic motivation in UTAUT theory, which explained the extent to which the activity of using IoT devices is perceived to be enjoyable, aside from any performance consequences resulting from technology use [57,59,63,67,72,73,76]. Furthermore, TAM's perceived ease of use and VAM's technicality are conceptually similar, and are associated with problems in usage [63,76]. Similarly, the perceived ease of use or perceived technicality have been tested extensively in the technology adoption literature, and refer to the degree to which a person believes that using the IoT or smart systems would be free of effort [44,50,52,53,57–60,63–65,67,68,70,73,76–78,111,135,136]. In addition, the "value" was identified in several studies as the benefits that could be derived from using a system [48,49,55,59,60,63,69,76]. Therefore, the value is the users' evaluation of the benefits to be derived from the IoT or smart devices against the cost of the device. Thus, the value provides the underlying direction to the individual's choice and/or their evaluation of the behavioral alternatives, which is adopted as a mediator in this study model, similar to the VAM concept [59,63,76]. Hence, the usefulness, enjoyment, and technicality are presumed to affect smart campus adoption.

Moreover, the perceived fee is one of the generic constructs in the VAM, and it is treated as the price value in UTAUT, and has subsequently appeared in the work of [4] as the cost of deployment. Accordingly, the cost of deploying smart programs should be straightforward to comprehend and quantify; of course, the cost of hardware and software licenses would rise when replicated on a larger scale. The cost is referred to as the unit cost which a consumer incurs by using IoT devices such as purchasing, installing, maintaining, and repairing the various components and devices of the IoT system [51,54,59,62–64,66–68,76,112,113], which has been tested to predict the technology adoption behavior. Similarly, existing studies using TAM and/or UTAUT approaches have discovered that trust is necessary for the acceptance of new digital technology [137–139]. Trust is described as the "willingness to rely" on the partner, which, in this case, is the IoT or smart devices [45,51,55,58,59,67,69–71,73,78]. However, the various foundations for trust and the varying levels of trust in societies are frequently overlooked. Thus, the fact that a sizable portion of the citizenry lacks trust and the existence of differences between cultures, cities, and nations are overlooked [140]. Privacy

and trust are widely regarded as multidimensional concepts, with various personal and contextual factors influencing people's perceptions [141]. Hence, privacy and security are adopted in the concept model as a single dimensional construct [4]. This is because privacy and security are related. The privacy is concerned with the right to select what personal information should be known to other people, and security focuses on how that information is protected from unauthorized access [4,43,45–48,55,59,60,66–68,70–73,112–114].

Securing data, infrastructure, and individuals' privacy is a challenge inherent in smart technology, and the smart campus is no exception [4]. Consideration should be given to protecting digital credentials for students, faculty, and staff, among others. A smart campus must have adequate security protocols and encryption mechanisms in place. Similarly, there is broad agreement on the importance of privacy, security, and trust as important criteria for IoT deployment and acceptance [125,142–145]. However, from the perspective of smart universities, empirical research focused on the implications of privacy, security, and trust remain insufficient. The effort of Chohan and Hu [78] has fallen short of addressing privacy and user trust; nonetheless, the security and trustworthiness of Internet of Things devices must be investigated in order to boost public trust. This research gap could provide universities with new insights into the full-scale use of IoT-based smart campuses, which would be particularly beneficial in developing countries. The success of IoT smart campus adoption in the future is thought to be dependent on the privacy, security, and trust of users. Hence, privacy and trust are related concepts that exhibit a range of preferences depending on the person and the context. However, current notice and consent procedures, most notably the use of privacy policies, do not adequately resolve customer privacy and trust preferences [141]. IoT systems implemented in public spaces as part of 'smart campus' initiatives present complicated privacy, security, and trust concerns. They pose complexities related to spatial implementation, alignment with existing systems, and a lack of clarity about data collection and usage practices. The concept presented in Figure 11 depicts how these typical elements may affect IoT-based smart campus adoption.

Thirdly, the concept of smart campus propagation was introduced by [4] to promote sustainability, which comprises several factors such as replicability, scalability, reliability, security and privacy, and the cost of deployment. The propagation is the ability of the smart campus to be replicated conveniently at various places or locations. Hence, the performance of smart campuses is contingent upon the model being easily replicable at different levels, ranging from academic departments to small communities to small cities and even consortia of cities. Numerous universities are housed in scattered buildings and have satellite campuses in distant geographical locations. This means that the structure of any smart campus model must promote its integration. Therefore, scalability, reliability, and replication are all planned factors of the conceptual model. The scalability describes how IoT-based smart campus solutions can adapt to the changes, or can be used in a range of capabilities. Hence, the scalability ensures that the system has the flexibility to address the needs of the users as they arise [4,146,147]. Similarly, the reliability factor ensures that there is no possibility of the IoT-based devices malfunctioning and not being able to provide the intended services, ensuring that they consistently operate properly and predictably [4,45,66,68,114]. At the same time, the replication is the ability of IoT smart devices to be repeated consistently and to obtain the same result [4,148,149].

Hence, the smart campus adoption model aims to propose a minimal model that can easily help relevant stakeholders understand the value of the smart campus initiative. The model's replication and scalability variables should be straightforward, demonstrating how the concept can be expanded with no or minimal development costs. Given that many smart campus programs can be directly replicated at the city level, these projects must be easily deployable at that level. When replicating the campus model in other locations, such as a town, city, or another campus, it is critical to protect the users' privacy. Still, understanding the potential cost will be essential for organizing and financing smart campuses. Similarly, the data produced should be trustworthy, and feedback from different sources should be checked before obtaining and filtering the data. Redundant hardware

is recommended when installed at critical facilities to ensure the data's integrity and, ultimately, the entire smart campus system. The replicability, scalability, security and privacy, reliability, trust, and cost of deployment are considered factors of propagation [4]. Moreover, any smart campus solutions should be easy to use, beneficial to the users, and enjoyable in order to add value to the system.

6. Conclusions

This study serves as a reference guide for smart campuses, emphasizing adoption patterns. As a result, this study proposes a solution to the lack of an adoption model for the smart campus initiative. In order to accomplish this, the researchers conducted a literature review, identified the commonalities among IoT adoption models that were suited for smart campus adoption, and developed a technology adoption model for smart campus adoption. In particular, the current study emphasized the crucial role that IoT-based smart campus adoption can play in the development of a sustainable campus environment. The research examines the major benefits and motives for establishing an IoT-enabled smart campus. A general overview of smart campus technology and applications is provided, emphasizing the importance of the adoption challenges that must be overcome to establish a sustainable smart campus. Hence, the present investigation discovered a range of models in the technology adoption or acceptance literature that can be used to improve technological adoption. According to the findings of this study, TAM and UTAUTs are the most prevalent models. On the other hand, the VAM model has lately gained popularity in the literature and has been adapted to investigate the adoption of the smart campus concept. Hence, the adoption model comprises security, privacy, and trust which are some of the challenges attracting discussion from several studies and are slowing the adoption and usage of IoT smart devices and applications. These factors affect the widespread, effective and efficient application and implementation of smart campus initiatives. At the same time, variables such as perceived scalability, replicability, reliability, security, trust, the cost of deployment, technicality, usefulness, and enjoyment are promising elements that could influence smart campus adoption.

Limitation and Future Work

The study presented a solution addressing the lack of a smart campus adoption model. The work is not without limitations. The selection of the papers focuses on the smart campus adoption concept linked to technology acceptance theories, but we realized that these categories of papers are severely limited. Thus, the focus was shifted toward IoT adoption to address the key objectives of this study, which is to propose a technology adoption theory for smart campuses. Future research can expand the inclusion criteria and other databases to see if more relevant studies could be identified. In the future, the researchers will focus on validating and verifying the conceptual framework introduced in this study. Moreover, future research may compare and prioritize the factors via AHP to select suitable factors to investigate the adoption of IoT-based smart campuses. The adoption model will help promote the concept of smart campuses, which is more sustainable and contributes to the development of a sustainable campus.

Author Contributions: This study was designed, directed and coordinated by Y.Y.J. and M.A.J. Y.Y.J., as the principal investigator, provided conceptual, financial, and technical guidance. M.A.J. assisted in planning the SLR and the data was analysed by R.S. and S.A. Moreover, R.S. generated and characterized the literature, while S.A. assisted in the organization and synthesis of the data. The manuscript draft was written by R.S., and commented on by all authors. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Technology Adoption Factors

Table A1. Constructs or factors from various theories/models.

Theoretical Models	Constructs	References
Technology Acceptance Models (TAM)	Perceived ease of use (PEoU), perceived usefulness (PU), behavioral intentions (BI), attitude, usage, mobile skills, social skills, information navigation skills, creative skills, IoT skills, perceived affective quality (PAQ), mobility, availability, trust, consumers' perceived innovativeness and intention to use, lack of sub-services, low network quality, low usability, low usefulness, low usage intention, alternatives, usage costs, personal information, personal formal, impersonal, privacy concern, perceived compatibility, vanity, need for uniqueness, perceived self-expressiveness, subjective norms or social influence, perceived behavioral control, security, familiarity, risk perception, perceived enjoyment, perceived connectedness, perceived cost, perceived system reliability, functionality and reliability, helpfulness, social network, community interest, product or service security, perceived risk, trust, IoT adoption, dimensions of national cultures	[44,45,47,50,52,57,58, 63–65,67–71,74,76,78]
Unified Theory of Acceptance and Use of Technology (UTAUT)	Performance expectancy (EE), effort expectancy (EE), social influence (SI), facilitating condition (FC), individual factors (IF), behavioral intention (BI), use behavior, technologically minded individuals, personal and societal benefits, society, mobility-related efficiencies, safety, technological and legal concerns, task technology fit (technology characteristics and task characteristics), awareness and self-efficacy, intention, data integrity, confidentiality, non-repudiation, authentication, availability, authorization, error, secondary use, collection, social influence trust, and enjoyment.	[47,53,56,63,73,76]
Theory of Planned Behavior (TPB)	Attitude, subjective norm, perceived behavioral control, and behavioral intentions.	[50,69]
Unified Theory of Acceptance and Use of Technology (UTAUT2)	Performance expectancy, effort expectancy, social influence, habit, facilitating conditions, behavioral intention (BI), environmental awareness, electricity-saving knowledge, use behavior, perceived fee, perceived enjoyment, and hedonic motivations.	[59,77]
Value-based Adoption Model (VAM)	Perceived fee, perceived technicality, purchase intention, behavioral intention, perceived privacy, perceived value, perceived trust, perceived health increase, and intention to use.	[59,63,76]
Theory of Reasoned Action (TRA)	Attitude, subjective norm, and behavioral intention (BI).	[50,69]
Motivation Opportunity Ability (MOA) Theory	Information quality, organizational support, users' self-efficacy, NFC value, satisfaction, reuse intention, expo satisfaction, and expo loyalty.	[49]
Innovation Diffusion Theory (IDT)	Compatibility, trialability, and observability,	[65]

Table A1. *Cont.*

Theoretical Models	Constructs	References
Self-Efficacy Theory (SE-theory)	Interpersonal influence, personal innovativeness, trustworthiness, attitude toward wearable, self-efficacy, health interest, perceived value, and intention to use.	[69]
Technology Organization Framework (TOE)	Perceived trustworthiness of technology, perceived benefits, perceived cost, external pressure, and IoT adoption intention	[51]
Influence Relationship Map (IRM)	Perceived utility, perceived expectancy, perceived usability, network externalities, adopting intention, domain-specific knowledge, user innovativeness, and usage behavior	[61]
Behavioral Reasoning Theory (BRT)	Value of openness to change, ubiquitous, relative advantage, compatibility, convenience, usage behavior, traditional barrier, risk barrier, attitudes towards the adoption of healthcare wearables, and adoption intention of IoT-based healthcare wearables	[60]
IoT-based Public Value Model (IoT-PVM)	System quality, information quality, service quality, PEoU, decision transparency, the trust of government, public trust, service collaboration, service effectiveness, service transparency, public engagement, PU, usage BI, and public value creation	[78]

References

1. Nord, J.H.; Koohang, A.; Paliszkiewicz, J. The Internet of Things: Review and theoretical framework. *Expert Syst. Appl.* **2019**, *133*, 97–108. [CrossRef]
2. Hsu, C.L.; Lin, J.C.C. Exploring factors affecting the adoption of internet of things services. *J. Comput. Inf. Syst.* **2018**, *58*, 49–57. [CrossRef]
3. Riggins, F.J.; Wamba, S.F. Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In Proceedings of the 2015 48th Hawaii International Conference on System Sciences, Kauai, HI, USA, 5–8 January 2015; pp. 1531–1540.
4. Min-Allah, N.; Alrashed, S. Smart campus—A sketch. *Sustain. Cities Soc.* **2020**, *59*, 102231. [CrossRef] [PubMed]
5. Pandey, J.; Singh, A.V.; Rana, A. Roadmap to smart campus based on IoT. In Proceedings of the 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 4–5 June 2020; pp. 909–913.
6. Haque, A.B.; Bhushan, B.; Dhiman, G. Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Syst.* 2021, *Early View*. [CrossRef]
7. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **2020**, *61*, 102360. [CrossRef]
8. Ahmed, V.; Abu Alnaaj, K.; Saboor, S. An investigation into stakeholders' perception of smart campus criteria: The American university of Sharjah as a case study. *Sustainability* **2020**, *12*, 5187. [CrossRef]
9. Valks, B.; Arkesteijn, M.H.; Koutamanis, A.; den Heijer, A.C. Towards a smart campus: Supporting campus decisions with Internet of Things applications. *Build. Res. Inf.* **2021**, *49*, 1–20. [CrossRef]
10. Valks, B.; Arkesteijn, M.; Koutamanis, A.; Den Heijer, A. Towards smart campus management: Defining information requirements for decision making through dashboard design. *Buildings* **2021**, *11*, 201. [CrossRef]
11. Valks, B. Smart Campus tools: Technologies to Support Campus Users and Campus Managers. Ph.D. Thesis, Delft University of Technology, Delft, The Netherlands, 2021.
12. Zeng, F.; Lee, S.H.N.; Lo, C.K.Y. The role of information systems in the sustainable development of enterprises: A systematic literature network analysis. *Sustainability* **2020**, *12*, 3337. [CrossRef]
13. Ghanem, M.; Elshaer, I.; Shaker, A. The successful adoption of is in the tourism public sector: The mediating effect of employees' trust. *Sustainability* **2020**, *12*, 3877. [CrossRef]
14. Alghamdi, A.; Shetty, S. Survey toward a smart campus using the internet of things. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 235–239.
15. Chuling, L.; Xie, Z.; Peng, P. A discussion on the framework of smarter campus. In Proceedings of the 2009 Third International Symposium on Intelligent Information Technology Application, Nanchang, China, 21–22 November 2009; Volume 2, pp. 479–482.
16. Liu, Y.L.; Zhang, W.H.; Dong, P. Research on the construction of smart campus based on the internet of things and cloud computing. *Appl. Mech. Mater.* **2014**. *543*, 3213–3217. [CrossRef]

17. Mattoni, B.; Pagliaro, F.; Corona, G.; Ponzo, V.; Bisegna, F.; Gugliermetti, F.; Quintero-Núñez, M. A matrix approach to identify and choose efficient strategies to develop the Smart Campus. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; pp. 1–6.

18. Muhamad, W.; Kurniawan, N.B.; Suhardi; Yazid, S. Smart campus features, technologies, and applications: A systematic literature review. In Proceedings of the 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 23–24 October 2017; pp. 384–391.

19. Hidayat, D.S.; Sensuse, D.I. Knowledge Management Model for Smart Campus in Indonesia. *Data* **2022**, *7*, 7. [CrossRef]

20. Alrashed, S. Key performance indicators for Smart Campus and Microgrid. *Sustain. Cities Soc.* **2020**, *60*, 102264. [CrossRef]

21. Liu, H. Smart campus student management system based on 5G network and Internet of Things. *Microprocess. Microsyst.* **2020**, *90*, 103428. [CrossRef]

22. Alam, T.; Alharbi, Y.M.; Abusallama, F.A.; Hakeem, A.O. Smart campus mobile application toward the development of smart cities. *Int. J. Appl. Sci. Smart Technol.* **2020**, *2*. [CrossRef]

23. Eltamaly, A.M.; Alotaibi, M.A.; Alolah, A.I.; Ahmed, M.A. IoT-Based Hybrid Renewable Energy System for Smart Campus. *Sustainability* **2021**, *13*, 8555. [CrossRef]

24. Pupiales-Chuquin, S.A.; Tenesaca-Luna, G.A.; Mora-Arciniegas, M.B. Proposal of a Methodology for the Implementation of a Smart Campus. In Proceedings of the Sixth International Congress on Information and Communication Technology, London, UK, 25–16 February 2021; Springer: Berlin/Heidelberg, Germany, 2022; pp. 589–602.

25. Chagnon-Lessard, N.; Gosselin, L.; Barnabé, S.; Bello-Ochende, T.; Fendt, S.; Goers, S.; Da Silva, L.C.P.; Schweiger, B.; Simmons, R.; Vandersickel, A.; et al. Smart Campuses: Extensive Review of the Last Decade of Research and Current Challenges. *IEEE Access* **2021**, *9*, 124200–124234. [CrossRef]

26. Abuarqoub, A.; Abusaimeh, H.; Hammoudeh, M.; Uliyan, D.; Abu-Hashem, M.A.; Murad, S.; Al-Jarrah, M.; Al-Fayez, F. A survey on internet of things enabled smart campus applications. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; pp. 1–7.

27. Anagnostopoulos, T.; Kostakos, P.; Zaslavsky, A.; Kantzavelou, I.; Tsotsolas, N.; Salmon, I.; Morley, J.; Harle, R. Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A Survey. *IEEE Access* **2021**, *9*, 131926–131954. [CrossRef]

28. Ceccarini, C.; Mirri, S.; Salomoni, P.; Prandi, C. On exploiting Data Visualization and IoT for Increasing Sustainability and Safety in a Smart Campus. *Mob. Netw. Appl.* **2021**, *26*, 2066–2075. [CrossRef]

29. Omotayo, T.; Awuzie, B.; Ajayi, S.; Moghayedi, A.; Oyeyipo, O. A Systems Thinking Model for Transitioning Smart Campuses to Cities. *Front. Built Environ.* **2021**, *7*, 755424. [CrossRef]

30. Awuzie, B.; Ngowi, A.B.; Omotayo, T.; Obi, L.; Akotia, J. Facilitating Successful Smart Campus Transitions: A Systems Thinking-SWOT Analysis Approach. *Appl. Sci.* **2021**, *11*, 2044. [CrossRef]

31. Durán-Sánchez, A.; Álvarez-García, J.; Del Río-Rama, M.; Sarango-Lalangui, P. Analysis of the scientific literature published on smart learning. *Espacios* **2018**, *39*, 14–27.

32. Molnar, A. Education in smart cities: Practices and challenges. In Proceedings of the IADIS International Conference Applied Computing, Utrecht, The Netherlands, 11–13 April 2019; pp. 256–260.

33. Rico-Bautista, D.; Medina-Cárdenas, Y.; Guerrero, C.D. Smart University: A Review from the educational and technological view of internet of things. In Proceedings of the International Conference on Information Technology & Systems, Quito, Ecuador, 6–8 February 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 427–440.

34. Molnar, A. Smart cities education: An insight into existing drawbacks. *Telemat. Inform.* **2021**, *57*, 101509. [CrossRef]

35. Musa, M.; Ismail, M.N.; Fudzee, M.F.M. A Survey on Smart Campus Implementation in Malaysia. *JOIV Int. J. Inform. Vis.* **2021**, *5*, 51–56. [CrossRef]

36. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [CrossRef]

37. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Keele, UK, 2007.

38. Hansen, E.G.; Schaltegger, S. The sustainability balanced scorecard: A systematic review of architectures. *J. Bus. Ethics* **2016**, *133*, 193–221. [CrossRef]

39. Qasem, Y.A.; Abdullah, R.; Jusoh, Y.Y.; Atan, R.; Asadi, S. Cloud computing adoption in higher education institutions: A systematic review. *IEEE Access* **2019**, *7*, 63722–63744. [CrossRef]

40. Ali, A.Q.; Sultan, A.B.M.; Abd Ghani, A.A.; Zulzalil, H. A systematic mapping study on the customization solutions of software as a service applications. *IEEE Access* **2019**, *7*, 88196–88217. [CrossRef]

41. Bukar, U.A.; Jabar, M.A.; Sidi, F.; Nor, R.N.H.B.; Abdullah, S.; Othman, M. Crisis Informatics in the Context of Social Media Crisis Communication: Theoretical Models, Taxonomy, and Open Issues. *IEEE Access* **2020**, *8*, 185842–185869. [CrossRef]

42. Ali, Z.H.; Ali, H.A. Towards sustainable smart IoT applications architectural elements and design: Opportunities, challenges, and open directions. *J. Supercomput.* **2020**, *77*, 1–58. [CrossRef]

43. Hsu, C.L.; Lin, J.C.C. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Comput. Hum. Behav.* **2016**, *62*, 516–527. [CrossRef]

44. De Boer, P.S.; Van Deursen, A.J.; Van Rompay, T.J. Accepting the Internet-of-Things in our homes: The role of user skills. *Telemat. Inform.* **2019**, *36*, 147–156. [CrossRef]

45. AlHogail, A. Improving IoT technology adoption through improving consumer trust. *Technologies* **2018**, *6*, 64. [CrossRef]
46. Jung, Y.; Park, J. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *Int. J. Inf. Manag.* **2018**, *43*, 15–24. [CrossRef]
47. Manfreda, A.; Ljubi, K.; Groznik, A. Autonomous vehicles in the smart city era: An empirical study of adoption factors important for millennials. *Int. J. Inf. Manag.* **2019**, *58*, 102050. [CrossRef]
48. El-Haddadeh, R.; Weerakkody, V.; Osmani, M.; Thakker, D.; Kapoor, K.K. Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement. *Gov. Inf. Q.* **2019**, *36*, 310–320. [CrossRef]
49. Han, H.; Park, A.; Chung, N.; Lee, K.J. A near field communication adoption and its impact on Expo visitors' behavior. *Int. J. Inf. Manag.* **2016**, *36*, 1328–1339. [CrossRef]
50. Mital, M.; Chang, V.; Choudhary, P.; Papa, A.; Pani, A.K. Adoption of Internet of Things in India: A test of competing models using a structured equation modeling approach. *Technol. Forecast. Soc. Chang.* **2018**, *136*, 339–346. [CrossRef]
51. Tu, M. An exploratory study of Internet of Things (IoT) adoption intention in logistics and supply chain management. *Int. J. Logist. Manag.* **2018**, *29*, 131–151. [CrossRef]
52. Caffaro, F.; Cremasco, M.M.; Roccato, M.; Cavallo, E. Drivers of farmers' intention to adopt technological innovations in Italy: The role of information sources, perceived usefulness, and perceived ease of use. *J. Rural Stud.* **2020**, *76*, 264–271. [CrossRef]
53. Ronaghi, M.H.; Forouharfar, A. A contextualized study of the usage of the Internet of things (IoTs) in smart farming in a typical Middle Eastern country within the context of Unified Theory of Acceptance and Use of Technology model (UTAUT). *Technol. Soc.* **2020**, *63*, 101415. [CrossRef]
54. Lin, D.; Lee, C.; Tai, W. Application of interpretive structural modelling for analyzing the factors of IoT adoption on supply chains in the Chinese agricultural industry. In Proceedings of the 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 10–13 December 2017; pp. 1347–1351.
55. Jayashankar, P.; Nilakanta, S.; Johnston, W.J.; Gill, P.; Burres, R. IoT adoption in agriculture: The role of trust, perceived value and risk. *J. Bus. Ind. Mark.* **2018**, *33*, 804–821. [CrossRef]
56. Yamin, M.A.Y.; Alyoubi, B.A. Adoption of telemedicine applications among Saudi citizens during COVID-19 pandemic: An alternative health delivery system. *J. Infect. Public Health* **2020**, *13*, 1845–1855. [CrossRef] [PubMed]
57. Choi, J.; Kim, S. Is the smartwatch an IT product or a fashion product? A study on factors affecting the intention to use smartwatches. *Comput. Hum. Behav.* **2016**, *63*, 777–786. [CrossRef]
58. Dutot, V.; Bhatiasevi, V.; Bellallahom, N. Applying the technology acceptance model in a three-countries study of smartwatch adoption. *J. High Technol. Manag. Res.* **2019**, *30*, 1–14. [CrossRef]
59. Niknejad, N.; Hussin, A.R.C.; Ghani, I.; Ganjouei, F.A. A confirmatory factor analysis of the behavioral intention to use smart wellness wearables in Malaysia. *Univers. Access Inf. Soc.* **2020**, *19*, 633–653. [CrossRef]
60. Sivathanu, B. Adoption of internet of things (IOT) based wearables for healthcare of older adults—A behavioural reasoning theory (BRT) approach. *J. Enabling Technol.* **2018**, *19*, 633–653. [CrossRef]
61. Kao, Y.S.; Nawata, K.; Huang, C.Y. An exploration and confirmation of the factors influencing adoption of IoT-based wearable Fitness trackers. *Int. J. Environ. Res. Public Health* **2019**, *16*, 3227. [CrossRef]
62. Kim, M.K.; Wong, S.F.; Chang, Y.; Park, J.H. Determinants of customer loyalty in the Korean smartphone market: Moderating effects of usage characteristics. *Telemat. Inform.* **2016**, *33*, 936–949. [CrossRef]
63. Pal, D.; Arpnikanondt, C.; Funilkul, S.; Chutimaskul, W. The Adoption Analysis of Voice-Based Smart IoT Products. *IEEE Internet Things J.* **2020**, *7*, 10852–10867. [CrossRef]
64. Park, J.H.; Kim, M.K. Factors influencing the low usage of smart TV services by the terminal buyers in Korea. *Telemat. Inform.* **2016**, *33*, 1130–1140. [CrossRef]
65. Nikou, S. Factors driving the adoption of smart home technology: An empirical assessment. *Telemat. Inform.* **2019**, *45*, 101283. [CrossRef]
66. Pal, D.; Papasratorn, B.; Chutimaskul, W.; Funilkul, S. Embracing the smart-home revolution in Asia by the elderly: An end-user negative perception modeling. *IEEE Access* **2019**, *7*, 38535–38549. [CrossRef]
67. Park, E.; Cho, Y.; Han, J.; Kwon, S.J. Comprehensive approaches to user acceptance of Internet of Things in a smart home environment. *IEEE Internet Things J.* **2017**, *4*, 2342–2350. [CrossRef]
68. Park, E.; Kim, S.; Kim, Y.; Kwon, S.J. Smart home services as the next mainstream of the ICT industry: Determinants of the adoption of smart home services. *Univers. Access Inf. Soc.* **2018**, *17*, 175–190. [CrossRef]
69. Hossain, M.I.; Yusof, A.F.; Che Hussin, A.R.; Iahad, N. Ali Safaa, S. Factors Influencing Adoption Model of Continuous Glucose Monitoring Devices for Internet of Things Healthcare. *Internet Things* **2021**, *15*, 100353. [CrossRef]
70. Dhagarra, D.; Goswami, M.; Kumar, G. Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. *Int. J. Med. Inform.* **2020**, *141*, 104164. [CrossRef]
71. Alraja, M.N.; Farooque, M.M.J.; Khashab, B. The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception. *IEEE Access* **2019**, *7*, 111341–111354. [CrossRef]
72. Park, C.; Kim, Y.; Jeong, M. Influencing factors on risk perception of IoT-based home energy management services. *Telemat. Inform.* **2018**, *35*, 2355–2365. [CrossRef]
73. Enaizan, O.; Eneizan, B.; Almaaitah, M.; Al-Radaideh, A.T.; Saleh, A.M. Effects of privacy and security on the acceptance and usage of EMR: The mediating role of trust on the basis of multiple perspectives. *Inform. Med. Unlocked* **2020**, *21*, 100450. [CrossRef]

74. Jaafreh, A.B. The effect factors in the adoption of Internet of Things (IoT) technology in the SME in KSA: An empirical study. *Int. Rev. Manag. Bus. Res.* **2018**, *7*, 135–148.

75. Won, J.Y.; Park, M.J. Smart factory adoption in small and medium-sized enterprises: Empirical evidence of manufacturing industry in Korea. *Technol. Forecast. Soc. Chang.* **2020**, *157*, 120117. [CrossRef]

76. Sohn, K.; Kwon, O. Technology acceptance theories and factors influencing artificial intelligence-based intelligent products. *Telemat. Inform.* **2020**, *47*, 101324. [CrossRef]

77. Alkawsi, G.A.; Ali, N.; Baashar, Y. An empirical study of the acceptance of IoT-based smart meter in Malaysia: The effect of electricity-saving knowledge and environmental awareness. *IEEE Access* **2020**, *8*, 42794–42804. [CrossRef]

78. Chohan, S.R.; Hu, G. Success factors influencing citizens' adoption of IoT service orchestration for public value creation in smart government. *IEEE Access* **2020**, *8*, 208427–208448. [CrossRef]

79. Rico-Bautista, D.; Guerrero, C.D.; Collazos, C.A.; Maestre-Gongora, G.; Sánchez-Velásquez, M.C.; Medina-Cárdenas, Y.; Swaminathan, J. Smart University: Key Factors for a Cloud Computing Adoption Model. In *Intelligent Sustainable Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 85–93.

80. Valks, B.; Blokland, E.; Elissen, C.; van Loon, I.; Roozemond, D.; Uiterdijk, P.; Arkesteijn, M.; Koutamanis, A.; Den Heijer, A. Supporting strategic decision-making on the future campus with space utilisation studies: A case study. *Prop. Manag.* **2021**, *39*, 441–465. [CrossRef]

81. Huang, L.S.; Su, J.Y.; Pao, T.L. A context aware smart classroom architecture for smart campuses. *Appl. Sci.* **2019**, *9*, 1837. [CrossRef]

82. Baudier, P.; Ammi, C.; Deboeuf-Rouchon, M. Smart home: Highly-educated students' acceptance. *Technol. Forecast. Soc. Chang.* **2020**, *153*, 119355. [CrossRef]

83. Kiryakova, G.; Angelova, N.; Yordanova, L. The potential of augmented reality to transform education into smart education. *TEM J.* **2018**, *7*, 556.

84. Singh, H.; Miah, S.J. Smart education literature: A theoretical analysis. *Educ. Inf. Technol.* **2020**, *25*, 3299–3328. [CrossRef]

85. Ahad, M.A.; Paiva, S.; Tripathi, G.; Feroz, N. Enabling technologies and sustainable smart cities. *Sustain. Cities Soc.* **2020**, *61*, 102301. [CrossRef]

86. Adamkó, A.; Kollár, L. Extensible data management architecture for smart campus applications-a crowdsourcing based solution. In Proceedings of the International Conference on Web Information Systems and Technologies, Barcelona, Spain, 3–5 April 2014; Volume 2, pp. 226–232.

87. Bosch, P.; Jongeneel, S.; Rovers, V.; Neumann, H.M.; Airaksinen, M.; Huovila, A. *CITYkeys Indicators for Smart City Projects and Smart Cities*; CITYkeys Report; Technical Research Centre of Finland: Espoo, Finland, 2017.

88. Kwok, L.f. A vision for the development of i-campus. *Smart Learn. Environ.* **2015**, *2*, 1–12. [CrossRef]

89. Malhotra, S.; Kumar, A.; Dutta, R. Effect of integrating IoT courses at the freshman level on learning attitude and behaviour in the classroom. *Educ. Inf. Technol.* **2020**, *26*, 1–15. [CrossRef]

90. Nie, X. Research on smart campus based on cloud computing and internet of things. *Appl. Mech. Mater.* **2013**, *380*, 1951–1954. [CrossRef]

91. Yu, S.J.; Sun, J.C.Y.; Chen, O.T.C. Effect of AR-based online wearable guides on university students' situational interest and learning performance. *Univers. Access Inf. Soc.* **2019**, *18*, 287–299. [CrossRef]

92. Papakostas, C.; Troussas, C.; Krouska, A.; Sgouropoulou, C. User acceptance of augmented reality welding simulator in engineering training. *Educ. Inf. Technol.* **2021**, *27*, 1–27. [CrossRef]

93. Al-Maroof, R.S.; Alfaisal, A.M.; Salloum, S.A. Google glass adoption in the educational environment: A case study in the Gulf area. *Educ. Inf. Technol.* **2020**, *26*, 1–24. [CrossRef]

94. Qashou, A. Influencing factors in M-learning adoption in higher education. *Educ. Inf. Technol.* **2021**, *26*, 1755–1785. [CrossRef]

95. Tavana, M.; Hajipour, V.; Oveisi, S. IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions. *Internet Things* **2020**, *11*, 100262. [CrossRef]

96. Sinha, N.; Singh, P.; Gupta, M.; Singh, P. Robotics at workplace: An integrated Twitter analytics–SEM based approach for behavioral intention to accept. *Int. J. Inf. Manag.* **2020**, *55*, 102210. [CrossRef]

97. Al-Nuaimi, E.; Al Neyadi, H.; Mohamed, N.; Al-Jaroodi, J. Applications of big data to smart cities. *J. Internet Serv. Appl.* **2015**, *6*, 1–15. [CrossRef]

98. Hashem, I.A.T.; Chang, V.; Anuar, N.B.; Adewole, K.; Yaqoob, I.; Gani, A.; Ahmed, E.; Chiroma, H. The role of big data in smart city. *Int. J. Inf. Manag.* **2016**, *36*, 748–758. [CrossRef]

99. Lo, J.H.; Lai, Y.F. The Study of using Augmented Reality Technique in Children's Natural Ecology Learning by Technology Acceptance Model. In Proceedings of the 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), Toyama, Japan, 7–11 July 2019; pp. 1045–1046.

100. Alqahtani, H.; Kavakli, M.; Sheikh, N.U. Analysis of the technology acceptance theoretical model in examining users behavioural intention to use an augmented reality app (imap-campus). *Int. J. Eng. Manag. Res.* **2018**, *8*, 37–49. [CrossRef]

101. Ashwin, T.; Guddeti, R.M.R. Impact of inquiry interventions on students in e-learning and classroom environments using affective computing framework. *User Model. User-Adapt. Interact.* **2020**, *30*, 1–43. [CrossRef]

102. Coccoli, M.; Guercio, A.; Maresca, P.; Stanganelli, L. Smarter universities: A vision for the fast changing digital era. *J. Vis. Lang. Comput.* **2014**, *25*, 1003–1011. [CrossRef]

103. Manqele, L.; Dlodlo, M.; Coetzee, L.; Williams, Q.; Sibiya, G. Preference-based Internet of Things dynamic service selection for smart campus. In Proceedings of the AFRICON 2015, Addis Ababa, Ethiopia, 14–17 September 2015; pp. 1–5.

104. Caţă, M. Smart university, a new concept in the Internet of Things. In Proceedings of the 2015 14th RoEduNet International Conference-Networking in Education and Research (RoEduNet NER), Craiova, Romania, 24–26 September 2015; pp. 195–197.

105. Roccotelli, M.; Mangini, A.M. Advances on Smart Cities and Smart Buildings. *Appl. Sci.* **2022**, *12*, 631. [CrossRef]

106. Owoc, M.; Marciniak, K. Knowledge management as foundation of smart university. In Proceedings of the 2013 Federated Conference on Computer Science and Information Systems, Krakow, Poland, 8–11 September 2013; pp. 1267–1272.

107. Tsai, I.C.; Yeh, C.H. Integrating SERVQUAL and Importance-Performance Analysis for Assessing Smart Campus Service Quality: A Case Study of an English Training Programme in Vietnam. In Proceedings of the 2015 IEEE 15th International Conference on Advanced Learning Technologies, Hualien, Taiwan, 6–9 July 2015; pp. 436–440.

108. Batty, M. Big data, smart cities and city planning. *Dialogues Hum. Geogr.* **2013**, *3*, 274–279. [CrossRef]

109. Chan, S.; Lu, M. Understanding internet banking adoption and use behavior: A Hong Kong perspective. *J. Glob. Inf. Manag.* **2004**, *12*, 21–43. [CrossRef]

110. Sun, H.; Zhang, P. The role of moderating factors in user technology acceptance. *Int. J. Hum. Comput. Stud.* **2006**, *64*, 53–78. [CrossRef]

111. Venkatesh, V.; Thong, J.Y.; Xu, X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Q.* **2012**, *36*, 157–178. [CrossRef]

112. Sharma, M.; Gupta, R.; Acharya, P. Prioritizing the critical factors of cloud computing adoption using multi-criteria decision-making techniques. *Glob. Bus. Rev.* **2020**, *21*, 142–161. [CrossRef]

113. Lanzini, F.; Ubacht, J.; De Greeff, J. Blockchain adoptioin factors for SMEs in supply chain management. *J. Supply Chain Manag. Sci.* **2021**, *2*, 47–68.

114. Paramita, R.A.; Dachyar, M. e alternative selection for internet of things (IoT) implementation in medical rehabilitation. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 3632–3640.

115. Dinev, T.; Hu, Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Inf. Syst.* **2007**, *8*, 23. [CrossRef]

116. Mofleh, S.; Wanous, M.; Strachan, P. The gap between citizens and e-government projects: The case for Jordan. *Electron. Gov. Int. J.* **2008**, *5*, 275–287. [CrossRef]

117. Jurcut, A.; Niculcea, T.; Ranaweera, P.; Le-Khac, N.A. Security considerations for Internet of Things: A survey. *SN Comput. Sci.* **2020**, *1*, 1–19. [CrossRef]

118. Sethi, R.; Bhushan, B.; Sharma, N.; Kumar, R.; Kaushik, I. Applicability of industrial IoT in diversified sectors: Evolution, applications and challenges. In *Multimedia Technologies in the Internet of Things Environment*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 45–67.

119. Sinha, P.; kumar Rai, A.; Bhushan, B. Information Security threats and attacks with conceivable counteraction. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; pp. 1208–1213.

120. Forbes Insight. *Internet of Things—From Theory to Reality*; Forbes Insight: Jersey City, NJ, USA, 2017.

121. Lund, D.; MacGillivray, C.; Turner, V.; Morales, M. *Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand*; Technical Report; International Data Corporation: Needham, MA, USA, 2014.

122. Gill, S.H.; Razzaq, M.A.; Ahmad, M.; Almansour, F.M.; Haq, I.U.; Jhanjhi, N.; Alam, M.Z.; Masud, M. Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study. *Intell. Autom. Soft Comput.* **2022**, *31*, 117–128. [CrossRef]

123. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]

124. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]

125. Sicari, S.; Cappiello, C.; De Pellegrini, F.; Miorandi, D.; Coen-Porisini, A. A security-and quality-aware system architecture for Internet of Things. *Inf. Syst. Front.* **2016**, *18*, 665–677. [CrossRef]

126. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]

127. Fernandez-Gago, C.; Moyano, F.; Lopez, J. Modelling trust dynamics in the Internet of Things. *Inf. Sci.* **2017**, *396*, 72–82. [CrossRef]

128. Guo, J.; Chen, R.; Tsai, J.J. A survey of trust computation models for service management in internet of things systems. *Comput. Commun.* **2017**, *97*, 1–14. [CrossRef]

129. Miloslavskaya, N.; Tolstoy, A. Internet of Things: Information security challenges and solutions. *Clust. Comput.* **2019**, *22*, 103–119. [CrossRef]

130. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of Things: Evolution and technologies from a security perspective. *Sustain. Cities Soc.* **2020**, *54*, 101728. [CrossRef]

131. Tornatzky, L.G.; Fleischer, M.; Chakrabarti, A.K. *Processes of Technological Innovation*; Lexington Books: Lexington, NE, USA, 1990.

132. Baker, J. The technology–organization–environment framework. In *Information Systems Theory*; University of Hamburg: Hamburg, Germany, 2012; pp. 231–245.

133. van Heck, S.; Valks, B.; Den Heijer, A. The added value of smart stadiums: A case study at Johan Cruijff Arena. *J. Corp. Real Estate* 2021, *ahead-of-print*. [CrossRef]

134. Valks, B.; Arkesteijn, M.; Den Heijer, A.; Vande Putte, H. Smart campus tools. Adding value to university goals by measuring real-time space use. *J. Corp. Real Estate* **2018**, *20*, 103–116. [CrossRef]

135. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User acceptance of information technology: Toward a unified view. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]

136. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]

137. Yeh, H. The effects of successful ICT-based smart city services: From citizens' perspectives. *Gov. Inf. Q.* **2017**, *34*, 556–565. [CrossRef]

138. Beldad, A.D.; Hegner, S.M. Expanding the technology acceptance model with the inclusion of trust, social influence, and health valuation to determine the predictors of German users' willingness to continue using a fitness app: A structural equation modeling approach. *Int. J. Hum. Comput. Interact.* **2018**, *34*, 882–893. [CrossRef]

139. Bahmanziari, T.; Pearson, J.M.; Crosby, L. Is trust important in technology adoption? A policy capturing approach. *J. Comput. Inf. Syst.* **2003**, *43*, 46–54.

140. Julsrud, T.E.; Krogstad, J.R. Is there enough trust for the smart city? exploring acceptance for use of mobile phone data in oslo and tallinn. *Technol. Forecast. Soc. Chang.* **2020**, *161*, 120314. [CrossRef] [PubMed]

141. Cottrill, C.D.; Jacobs, N.; Markovic, M.; Edwards, P. Sensing the City: Designing for Privacy and Trust in the Internet of Things. *Sustain. Cities Soc.* **2020**, *63*, 102453. [CrossRef]

142. Marias, G.F.; Barros, J.; Fiedler, M.; Fischer, A.; Hauff, H.; Herkenhoener, R.; Grillo, A.; Lentini, A.; Lima, L.; Lorentzen, C.; et al. Security and privacy issues for the network of the future. *Secur. Commun. Netw.* **2012**, *5*, 987–1005. [CrossRef]

143. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]

144. Gessner, D.; Olivereau, A.; Segura, A.S.; Serbanati, A. Trustworthy infrastructure services for a secure and privacy-respecting internet of things. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 998–1003.

145. Ransbotham, S.; Fichman, R.G.; Gopal, R.; Gupta, A. Special section introduction—Ubiquitous IT and digital vulnerabilities. *Inf. Syst. Res.* **2016**, *27*, 834–847. [CrossRef]

146. Sun, P.; Kretzschmar, H.; Dotiwalla, X.; Chouard, A.; Patnaik, V.; Tsui, P.; Guo, J.; Zhou, Y.; Chai, Y.; Caine, B.; et al. Scalability in perception for autonomous driving: Waymo open dataset. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 2446–2454.

147. Gupta, A.; Christie, R.; Manjula, P. Scalability in internet of things: Features, techniques and research challenges. *Int. J. Comput. Intell. Res* **2017**, *13*, 1617–1627.

148. Sun, X.; Wang, G.; Xu, L.; Yuan, H. Data replication techniques in the Internet of Things: A systematic literature review. *Libr. Hi Tech.* **2021**, *ahead-of-print*. [CrossRef]

149. Naas, M.I.; Lemarchand, L.; Raipin, P.; Boukhobza, J. IoT Data Replication and Consistency Management in Fog computing. *J. Grid Comput.* **2021**, *19*, 1–25. [CrossRef]