technologies

MDPI

Article

Improving IoT Technology Adoption through Improving Consumer Trust

Areej AlHogail

Information Systems Department, Al Imam Mohammad Ibn Saud Islamic University, Riyadh 12722, Saudi Arabia; aalhogail@imamu.edu.sa; Tel.: +966-1-1259-7688

Received: 24 May 2018; Accepted: 5 July 2018; Published: 7 July 2018

Abstract: Studies have shown that trust plays a crucial role in the consumers' decision to adopt Internet of Things (IoT) technologies and services since it helps them to overcome perceptions of risk and uncertainty related to it and enhances the customers' level of acceptance and adoption intention. Nevertheless, the literature of IoT still lacks studies on the behavioral aspect that explain the customers' perception towards IoT adoption and focuses more on technological aspect. The main goal of this study is to examine the factors that influence consumer trust and their role in the adoption of IoT technology. A conceptual trust model that encompasses the major factors affecting trust towards IoT technology adoption has been presented. The model is composed of three dimensions of factors that we assume will influence the level of trust which are: product related factors, social influence related factors and security related factors. This framework is validated through surveying consumers' opinions, which provide views and feedback regarding factors influencing their trust towards this technology. The model can assist researchers to further investigate the trust issues and create a trustworthy literature to guide IoT products' development and marketing strategies that are focused on the consumer's requirements.

Keywords: Internet of Things (IoT); trust; adoption; information security; human behavior

1. Introduction

The Internet of Things (IoT) has gained huge importance in recent years as it aims to provide people with innovative and intelligent technologies and services, in which all of the physical objects around them are linked to the Internet and are able to communicate with each other. IoT products and services span several fields, including healthcare, hospitality, transport, infrastructure, education, and social services. Smart devices that are often interconnected with cloud services provide easy and global access and lead more consumers to engage in such technology.

An IoT system can be described as a collection of interconnected smart devices and objects that are provided with unique identifiers that are able to communicate and transfer data without human or computer interaction in order to fulfill a desired goal. It embraces a variety of technologies, services, and standards [1]. IoT involves people, objects and data as major agents. It is expected that more than tens of billions of objects are expected to be a part of this network by the year 2030 [2,3].

Different security challenges could face the adoption of the IoT. Sicari et al. [1] have listed some of the most important challenges. First, data anonymity, confidentiality and integrity are desirable to ensure the basic security concerns of consumers. Moreover, access controls, which control authentication and authorization, is required to prevent unauthorized access to the system. In addition, privacy requirements should be enforced to ensure users' personal information confidentiality and data protection. In addition, trust is an essential concern since the IoT environment consists of different devices that have to process and handle user data. This paper is concerned with the last challenge mentioned, namely trust.

IoT needs to collect and deal with unprecedented volumes of private, real-time and detailed data. Nevertheless, personal data is always a sensitive subject and consumers usually are cautious about sharing data for fear that it can be used in any inappropriate ways. Undeniably, with this high level of heterogeneity, combined with the wide scale of IoT technology and the increased intractability of people and machines, it is expected to expand security threats. Moreover, the traditional security and privacy countermeasures cannot be directly applied to IoT systems due to several challenges such as their limited computing power, the high number of interconnected devices and scalability issues. Establishing trust for IoT technologies that are spread across discrete settings and that are large scale is a great challenge for end consumers. Devices, back end systems and data repositories might also be vulnerable to physical and security attacks. Furthermore, the networks that carry the transmitted data are untrusted and might be subject to attacks. Concurrently, to reach user acceptance and adoption, it is required to set valid security, privacy and trust models that are suitable for the IoT systems [1,4].

An IoT product such as a smart home application will use different sensors to control the room smartly and remotely and will collect data from very sensitive and private domains, such as a bedroom. Nonetheless, this is an automated communication in which the user takes no active role [5]. In such a situation, security, and, in particular, trust remain major challenges for consumers and developers of IoT application and services. The ignorance of such issues could lead to undesired consequences such as lack of trust, non-acceptance, and damage to reputation [2].

Although consumers believe that the IoT has the potential to benefit them, they will always be concerned about their data security and privacy and any potential data breach. The opportunities provided by interconnected IoT devices are usually accompanied by many security and privacy issues. It is found that trust can be perceived as a significant factor that influences behavioral intention to use an IoT technology and has a strong effect in comparison to other concerns such as privacy [6]. Falcone and Sapienza [7] stated a number of reasons why users might not grant high trust levels, as they might fear that a task is not carried out as expected or it is not accomplished at all, or even that damage is caused. Therefore, an IoT system must possess a series of characteristics, such as encryption and usefulness, in order to be trusted and accepted by users. This paper aims to identify the major characteristics needed for an IoT device or a service to be trusted by consumers.

The success of the IoT essentially depends on the consumer perceptions about IoT products' security and the level of their trust [2]. Moreover, good participation is usually related to a high enough level of trust [8]. In the global rush to promote IoT technologies, the industry is lagging behind on investing in consumer trust. Nonetheless, the consumer's adoption is greatly dependent on establishing their trust. Most previous research on this concept has concentrated on the technical issues of IoT usage but neglected the IoT users and their perceptions about the technology [8,9]. Consequently, a deep understanding of the factors that lead to customers' trust in IoT-enabled products and services could help developers to implement efficient and widely adopted IoT services [10]. Different studies, such as [2,11,12], have presented various dimensions as influencers of trust; however, each study has put forth different factors.

This study presents a comprehensive review of the different factors that affect consumers' trust of IoT services and products. Moreover, this paper proposes and tests a conceptual model of the collected factors. The model is based on three major hypotheses: product-related factors have a positive influence on trust towards IoT technology adoption; social influence-related factors have a positive influence on trust towards IoT technology adoption; and security of products and services-related factors have a positive influence on trust towards IoT technology adoption. Consequently, the level of trust in the IoT technology is positively associated with the adoption of IoT. This study aims to identify specific factors under each category that could influence the trust decision. This model could be used to inform future research directions and aid developers in understanding the related factors that could affect IoT adoption decisions. In addition, these factors would be valuable for the implementation of development and marketing plans that are based on consumers' requirements.

The structure of the paper is as follows: first, a literature review is presented to emphasize the significance this research topic. Second, the conceptual model and a description of the data analysis are presented to validate the introduced model. Finally, the results and conclusion of the study are discussed.

2. Literature Review

The Internet of Things (IoT) has become an exploration focus for both industry and academia. The features and capabilities that are offered by the IoT are the main motivations of gaining significant attention in both fields [13]. It is also related to several human-related factors. The IoT enables the creation of a network of connected objects around us that communicate with each other with minimal human involvement [13]. The IoT consists of four levels. The first is a perception layer composed of different sensors and data collectors, followed by a network layer that controls the transmission of the data. The next layer is the middleware layer, which involves the information processing systems. Finally, the fourth level is the application and services level [14].

IoT manufacturers are investing in additional intelligence and interconnectivity among devices; however, security and privacy concerns are poorly reflected in the development, as represented by, for instance, poorly encrypted or unencrypted communications, defective user interfaces, or weak passwords that expose the consumers and their private data to potential attacks [2]. Moreover, the concept of privacy is very often related to trust. By preserving privacy, consumers will be able to determine whether, when, and to whom their personal information is to be released or disclosed [15]. The IoT product or service must preserve its users' privacy to be able to attain their trust. However, many IoT products pay less attention to these critical factors due to the high cost of security and limited resources. The "2018 Global Data Threat Report" disclosed that around 71% of surveyed organizations are aggregating data from millions of IoT devices in use [16]. Nevertheless, consumer trust is very important to making an adoption decision.

Trust is a complex concept that is affected by numerous assessable and non-assessable variables [15]. It is interrelated to security, as guaranteeing system security and user safety is essential to gaining trust. Trust embodies beliefs that a system has the necessary elements to perform as expected in different conditions [17]. Mayer el al. [18] defined trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p. 172). The latest technology adoption research has focused on trust as a critical driver of technology usage behaviors [19].

In the IoT, trust is a process that is initiated by the user based on his/her evaluation and expectation of the IoT product's competence, and involves the user deciding to delegate to or rely on the trusted entity to fulfill a desired goal. The user would accept all the risks of becoming vulnerable that are associated with this trust relationship [8]. In the IoT, trust could be considered as vital for consumer adoption [20] because it can deal with two critical situations of IoT systems, namely, uncertainty and risk of vulnerability [10], as consumers must be able to interact with interconnected IoT devices and systems safely, reliably, and intuitively. Only trust is what makes people use such devices, despite all of the possible risks and the need to overcome perceptions of uncertainty and risk. Moreover, trust helps users to distinguish trustworthy products and technologies from the malicious ones [7].

Trust is essential to encourage people to easily adopt modern technology despite unpredictable circumstances. In uncertain situations, trust assists the individual to understand the social surroundings of the technology and decreases vulnerability [18]. Thus, trust is considered to be a serious factor in studies concerning online services. Research of human behavior online has highlighted the significance of embracing trust in adoption models to understand success factors behind consumer acceptance and adoption of IoT products and services [10]. For instance, the study by Gao and Bai [11] concluded that trust has significant effects on the behavioral intention to adopt IoT products and services. Han et al. [21] proved that trust is an essential factor for the adoption of third-party

applications. Therefore, trust is very critical to the adoption of IoT products due to the aforementioned reasons, rendering the spread of IoT systems very difficult without users' trust [7]. In this paper, we investigate IoT technology adoption and identify the factors that influence this adoption. Technology adoption is the process that begins with the user awareness of the technology, and finishes with embracement and full use of that technology [22].

The literature on the technical aspects of the IoT is more extensive than that on the behavioral and attitudinal aspects. The literature lacks effective trust models or frameworks to elucidate and guide IoT technology designers and service providers of the requirements of the users and the associated risks that are hard to understand and manage. The literature and industry are more focused on connectivity, distant controlling, and other IoT device features. Trust models that clarify consumers' requirements and service providers' responsibilities are required to ensure that people can use IoT technologies with less concern. This indicates the need for more investigation in that field.

Few studies have investigated the role of trust in IoT adoption—for example, see References [10,11,20,23–25]. Most of these studies have focused on the Technology Acceptance Model (TAM) model and identified trust as one factor towards technology acceptance. Gao and Bai [11], Al-momani et al. [9] and Coughlan et al. [23] considered trust as one enabler of the IoT adoption intention. Khan et al. [2] designed a trust model that is based on two main factors to enable consumer trust namely: security and privacy. Yan et al. [15] discussed a trust management framework that is system architecture designed to achieve trust management based on the different levels of the IoT structure. The Lin and Dong [8] trust model is based on the relationship between the major ingredients, namely: trustor, trustee, goal, trustworthiness evaluation, decision, action, result, and context. However, these models do not directly cover the behavioral factors that impact the trust factor in order to influence the consumer adoption intention decision. Therefore, this study aims to contribute to the body of knowledge in this field and to fill this research gap by specifying the factors that influence the consumer trust decision.

3. Conceptual Model and Research Hypotheses

This section presents the proposed IoT technology trust model. It begins with describing the structure of the conceptual model and emphasizes the scope of the model, as it is capable of accommodating a number of factors associated with consumer intention to trust. This is followed by a description of the details of each of the dimensions and a presentation of the research hypotheses.

3.1. IoT Technology Trust Model

Lee and Turban [26] summarized the theoretical perspectives in trust-related studies into three categories:

- Personality theory is based on characterizing trust as a belief genuinely rooted in behavior and as initiating in the personality's initial psychological development.
- In sociology and economics, trust is described as a phenomenon within and between groups, organizations and/or individuals' trust put in them.
- Social psychology conceptualizes trust as the expectations and willingness of the trusting party in a transaction, the threats accompanying such a transaction, and the related factors that either improve or hinder the development and preservation of that trust.

The social-psychological perspective seems to be the most appropriate for studying factors affecting consumer trust in IoT because it focuses on transactions, as well as on the situations of uncertainty, which are usually associated with IoT transactions. To understand the significance of the trust factors on the adoption of IoT technology, a research conceptual model has been proposed that draws from the diverse research on trust and is based theoretically on the social-psychological perspective and the technology acceptance model (TAM).

Technology acceptance model (TAM) is an information systems common theory that models the way a user accepts and uses a technology. It mainly focuses on the impact of attitude on behavior [27]. Researchers have verified and validated the TAM, which has been shown to be suitable as a theoretical foundation for the adoption of technology [28]. The TAM proposes that there are many factors influencing users' decisions regarding how and when they will use a system recent presented to the field. In particular, the TAM suggests that the two key elements of behavioral intention to use a new technology are perceived ease of use and perceived usefulness [11].

The proposed model's factors correspond to the TAM factors in two main ways. Firstly, in the TAM, the user intention to adopt technology is usually affected by external factors. In this model, the trust that leads to adoption is based on a number of external factors. Moreover, the two major factors from TAM, namely perceived ease of use and perceived usefulness, were employed as the starting points to collect other factors that can influence trust towards adoption.

Different factors collected from the literature were combined to form the model based on social-psychological perspective. This perspective aims to aid in the understanding of individual behavior in a social context, as well as how it could be influenced by other people and the social context. The conceptual model guiding this research is illustrated in Figure 1.

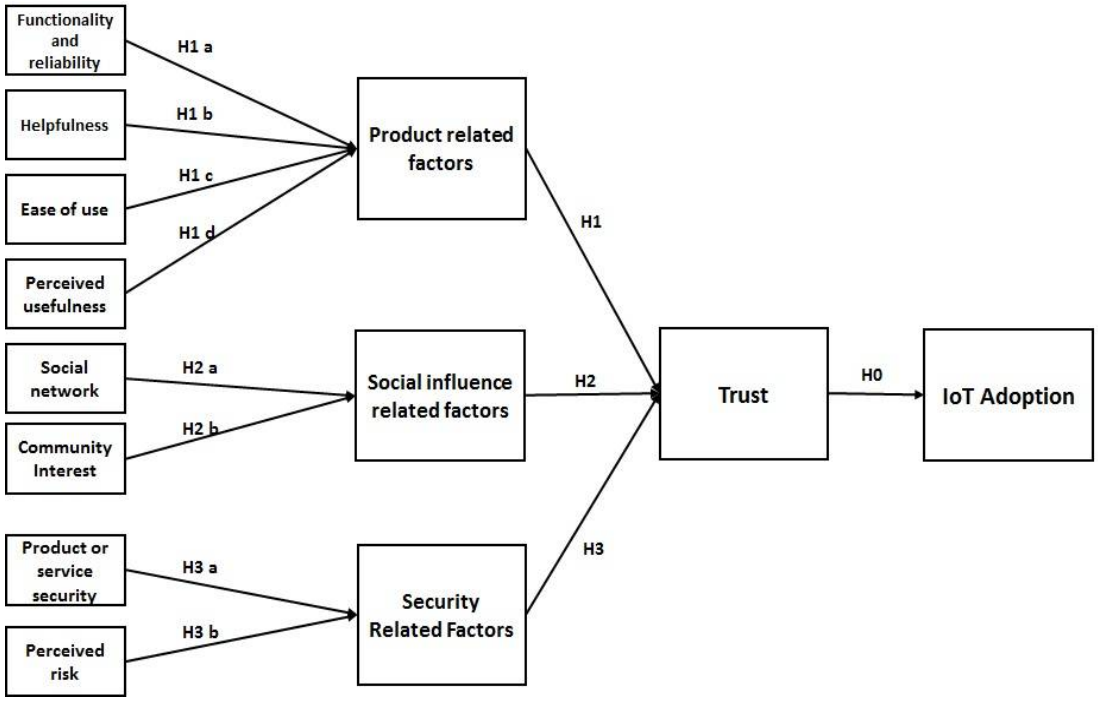

Figure 1. IoT technology trust model.

3.2. *Trust Related Factors and Research Hypotheses*

Trust is impacted by numerous quantifiable and non-quantifiable factors. The conceptual model classified the factors into three main dimensions, namely: product-related factors, social influence-related factors and security-related factors. Each dimension consists of a number of factors.

3.2.1. Product-Related Factors

A number of factors that are product-specific could influence the consumer decision to trust an IoT product or service. Different models and studies have suggested a number of product-related factors that could influence trust and thus affect the adoption decision. Based on the literature, a number of factors have been collected as listed below.

Functionality and reliability refer to whether a technology has the capacity or ability to perform a specific task by providing required features and functions, and whether it will consistently operate properly and predictably [17]. It must have the capacity to detect data corruption and try to fix it. This feature is essential for IoT products and services to keep running efficiently and securely.

Technology's functionality trust depends on its ability to perform correctly. It is noted that consumers' trust is based on perceiving that the product or service will perform its proposed and required functions [29]. Moreover, reliability will have a positive influence on trust in the adoption of IoT, as reported by Tam et al. [19,29]. Because errors are not acceptable to end-users, there is a huge impact of the absence of errors on trust towards IoT adoption [30]. Thus, the first hypothesis is:

H1A. *IoT technology functionality and reliability have positive effects on trust towards its adoption.*

Helpfulness refers to the technology's support and ability to provide adequate, effective, and responsive advice that may be necessary to complete a task—including instructions, guidelines, and help pages [17,19]. People may not fully utilize technology, as they may fear that they will not find the appropriate support if things go wrong. This may limit the benefits of the technology and usually will affect the adoption of the technology [17,19]. Providing such support to users can guide them by avoiding undesired surprises. Moreover, users who trust the support that is offered to them might perceive themselves to be more capable of using the system successfully. For instance, if a user trusts the interactive guidance of a system, they may believe that they are more likely to use it effectively, leading to their adoption of that system [5]. Therefore, we can conclude that, in order to gain better trust that leads to IoT adoption, good investment in providing support for end-users is crucial. Hence, we will assume that:

H1B. *IoT technology helpfulness has a positive effect on trust towards its adoption.*

Ease of use discusses the degree to which a user considers that using a specific technology would be effort free. According to Lai et al. [29], a technology's ease of use plays a noteworthy role in building up the trust of users towards this technology. Usually, the ease of use or usability is affected by how accessible the system is to the users and how the interaction is designed. For example, the user should be able to use it correctly with a minimal chance of making mistakes [31]. This in turn usually affects the trust towards IoT adoption [29]. Studies have revealed that a high usability of IoT products or services increases the satisfaction level of end-users and affects the adoption intention [11].

Different researchers have emphasized the positive effect of ease of use towards improving the trust that leads to IoT adoption. For example, Gao and Bai [11] found that perceived ease of use has a major effect on IoT services adoption. Similar findings were reported by Abu et al. [32], showing that ease of use is one of the most important factors for adoption. Consumers tend to trust commonly used IoT products and services and distrust cases that are perceived to be outside their control [12]. Thus, it is expected that the perceived ease of use has a significant effect on trust toward IoT adoption.

H1C. *Perceived ease of use has a significant effect on trust towards IoT technology adoption.*

Perceived usefulness refers to the degree that a user believes that the system usage would enrich their performance and lifestyle [17]. Different researchers have indicated the positive relationship between IoT products or services adoption rates and the perception of consumers that the technology would facilitate their daily life [11]. The satisfaction level of consumers affects their trust, which leads to the intention to adopt IoT technologies. Perceived usefulness was found to be an important influencer of the intention to adopt IoT technology in different studies [6,23]. The TAM specifies that perceived usefulness is a major element of behavioral intention to the adoption of new technology [9,28]. Moreover, the perceived usefulness of IoT services advocates that individuals will feel that such services will enable them to enhance their overall performance in everyday situations [11]. Therefore, the perceived usefulness of the IoT technology must be advocated to achieve a successful adoption. Therefore, we assume that:

H1D. *Perceived usefulness has a strong effect on trust towards IoT technology adoption.*

3.2.2. Social Influence-Related Factors

In the case of IoT technology or service adoption, most users lack reliable information about product details, which could help them to make a decision. Social influence is demonstrated as a person's perception of a product or a service that is highly influenced by the perceptions of others. The Unified Theory of Acceptance and Use of Technology (UTAUT) considered social influence as one of four factors that influence consumers' technology adoption. Gao and Bai [11] and Abu et al. [32] found a positive influence of social-related factors on the adoption of IoT technology. Social influence has gained extensive attention in the information systems field [33]. In this study, we divided social influence into two precise factors: social network and community interest.

The social network individual social network refers to the notion that opinions and evaluations of a product will influence the individual decision on that product. Therefore, the model should incorporate social influence as an influencing factor. It is demonstrated by a person's perception of whether other significant people in their community perceived that they should engage with this technology or service [11]. Social networks play a crucial role in influencing the user adoption of IoT technology since users generally seek information from peers, family, and even social media influencers' reviews to reduce IoT product or service uncertainty prior to purchase [33]. Users usually trust relevant users' reviews and opinions since these reviews can be taken as trusted evaluations of a product. As Gao and Bai [11] stated, numerous consumers have considered mobile IoT devices to be trustworthy since these devices have trended on their social networks [11,33]. However, customers tend to doubt or resist the reviews and evaluations by developed companies. Thus, social networks play a significant role in influencing consumer trust toward IoT adoption and must be taken into account when introducing IoT products or services into the market [8]. Therefore, it is hypothesized:

H2A. *Consumer's social network has a positive influence on trust towards IoT technology adoption.*

Community Interest. Community interest is an important factor that empowers trust and interaction between objects of the same community [34]. Community interest and culture could highly affect how individuals make their decisions. Although globalization has enabled the world to grow closer, cultural differences still can distinguish nation from nation. For instance, a conservative Middle-Eastern culture could react differently to video-camera sensors than less conservative cultures. Managing trust requires an in-depth investigation of the local market, as domestic culture might create barriers, in addition to national legislation. National differences might have a positive or a negative effect on trust in any new technology [35,36]. It is also important to note that sometimes the lack of alternatives or necessity could influence that factor towards trust [12]. Nevertheless, there is a lack of studies on the impact of culture on trust [36]. Consequently, it is evident that, for any new IoT technology or service entering a new market, the local community interest must be taken into the account and a deep investigation and appreciation of the local perceptions and opportunities related to trust must be conducted. Thus, it is hypothesized:

H2B. *Community interest has a positive influence on trust towards IoT technology adoption.*

3.2.3. Security-Related Factors

Security in this context indicates the extent to which a user considers that using an IoT product or a service would be risk-free. Security is a major concern of customers adopting a new product or service, and it has a noteworthy impact on consumer trust of a specific product or service, and therefore on the adoption of the given technology [6,7,9,26]. In order to increase adoption, consumers should feel safe when using these systems. Moreover, lack of security was found to be a major issue that prevented customers from adopting the IoT services [9]. To achieve trust though product security,

several factors need to be taken care of. We have divided these factors into product (trustee) security and perceived risks.

Product or service (trustee) security. This factor is concerned with the ability of the trustee to achieve major security concerns such as confidentiality, integrity, and availability. This factor could be affected by trustee reputation and earlier behaviors and performance [15]. Security is usually considered a critical concern to consumers when it comes to trust towards adoption [29]. The level of security and privacy are critical characteristics of IoT technology that affect the development of consumers' confidence in them, as they gives the consumer the assurance that they will be safe [29].

There are several security goals that should be achieved, namely:

- Confidentiality assures that the sensitive data collected through IoT devices is accessed or viewed only by authorized entities.
- Availability guarantees the survivability of IoT services despite attacks.
- Integrity guarantees that the content of the transmitted data, to and from IoT devices, is in its original form.
- Authenticity facilitates an IoT device to confirm the identity of the other device that it is interacting with.

According to Koien [12], users tend to trust IoT devices that enable identity authentication and access control. Devices that show the capability and readiness to be protected are more noted to be trusted. Therefore, we can conclude that there is a positive relationship between trust and IoT product or service security level.

H3A. *Product or service's security has a positive impact on trust towards IoT technology adoption.*

The perceived risks associated with a product or service. In the IoT context, the perceived risks are higher due to the distinctive characteristics of IoT products and services such as low computing resources and sometimes a reduced encryption level. Thus, consumers feel more uncertainty and risk in their adoption decision [6,11,29,37]. Trust is considered an effective variable for decreasing uncertainty and creating a sense of safety [11], and consequently, trust plays a major role in adoption intention. Consumers tend to distrust IoT devices or services that they perceive to be outside of their control, as such devices or services are assumed to carry a too high of a risk [12]. There is an incompatibility between the actual risk level and the person's trust in IoT technology that is usually built upon the perceived risk [12]; therefore, we separated the actual product or service security level and the perceived risk. However, there is an inverse relationship between the actual product security level and the perceived risk associated with that product or service.

H3B. *Perceived risk associated with IoT technology has a positive influence on trust towards IoT technology adoption.*

4. Methodology

4.1. Data Gathering

A survey was conducted to validate the model by establishing the consensus of attitudes from a wide range of consumers that have used IoT technology before. The survey was collected during the months of November and December 2017, through using an online survey to reach a higher number of users. Since IoT technologies have a varied range of products and services, concentrating on a specific IoT product would enrich the exactitude of this study [11]. Therefore, the focus was on home/domestic-use IoT devices such home-controlled surveillance devices, smart appliances, and smart televisions.

The questionnaire was composed of two sections. In the first section, demographic information was useful to segment the data and compare the respondents. This section gathered information regarding age group, gender, income, education level, English language proficiency, and IoT technology

familiarity. The purpose of the second section was to assess the factors affecting trust based on the conceptual model factors. It contained three sets of questions, which represented the three main dimensions of factors and were related to a total of eight factors of the trust model. Each factor was represented by several demonstrative statements in order to be evaluated. After that, approved statements were analyzed as clusters to evaluate each dimension of factors and their relation to one another [38]. The survey helped the researchers to identify the key factors and to evaluate which factors were perceived as more significant than others. The statements were divided into groups to cover the following hypotheses, as described in Table 1.

Table 1. The survey questions' description.

Dimension Hypotheses	Domain Hypotheses	Description of Survey Questions
H1 product-related factors have a positive influence on trust towards IoT technology adoption	H1A IoT technology functionality and reliability have a positive effect on trust towards its adoption	To study the effect of availability of clear information regarding the IoT product functionality and reliability on consumer trust. Moreover, it measures the effect of the consumer expectancy of product functions, quality and capabilities towards user decision of adoption.
	H1B IoT technology helpfulness has a positive effect on trust towards its adoption	To assess the application of different efficient and clear guidance and support on the behaviour and attitude of consumers trust towards adoption.
	H1C perceived ease of use has a significant effect on trust towards IoT technology adoption	To study the influence of product ease of use and product design on increasing product trust and affect consumer decision about product adoption
	H1D perceived usefulness has a strong effect on trust towards IoT technology adoption	To study the impact of perceiving that using IoT devices/products will makes consumer life easy and smart and save time and effort on his/her decision of adoption
H2 Social Influence related factors have a positive influence on trust towards IoT technology adoption	H2A a consumer's social network has a positive influence on trust towards IoT technology adoption.	To assess the influence of product reviews on different evaluation platforms, such as social networks, and friends and relatives on consumer decision to buy and use a new IoT product
	H2B community interest has a positive influence on trust towards IoT technology adoption.	To evaluate the role of culture and community interest on consumer trust and adoption decision including respecting local culture.
H3 Security of products and services related factors have a positive influence on trust towards IoT technology adoption	H3A product or service's security has a positive influence on trust towards IoT technology adoption.	To study the importance of taking care of IoT product security and privacy in influencing consumer trust in the product and purchasing decision
	H3B perceived risk associated has a positive influence on trust towards IoT technology adoption	To assess the effect of user perception that the product could risk his/her privacy or security on IoT product adoption

Respondents were inquired to indicate each statement significance level to trust towards IoT adoption. The questionnaire used a five-point Likert scale in order to assess the respondent's degree of agreement with each statement. The five-point Likert scale was employed to help avoid bias.

A total of 400 responses were received. Then, the acquired data were arranged for analysis. The data preparation included the process of removing any missing values from the dataset and ensuring that the data was not significantly distorted by dissimilar views. The *t*-test was applied to address the possible non-response bias, as embraced by Lau et al. [11], in order to compare the average means

of the key variables of the last and first 10% of the responses. The *t*-test results indicated the lack of significant difference among the response groups. Hence, a non-response bias was determined.

4.2. Results and Analysis

The data collected through the survey were quantitatively analyzed through two steps. Firstly, the model reliability and validity were tested and then the conceptual model was examined through statistical analysis to test the research hypotheses and model fitness. A non-parametric test was applied when applicable, since the data was ordinal and small in size.

In relation to respondents' ages, the majority (35.5%) were between 20 and 30 years old; followed by 27.5% were between 30 and 40 years old; 17% percent were aged below 20; 13% were aged between 40 and 50; and those who were aged over 50 years old represented 7.5% of the responses. Regarding the education level, 13% were high school graduates or less qualified; 58% had completed a bachelor degree; and 24% held a postgrad degree. In regards to English proficiency, 44% of the respondents had intermediate English proficiency, whereas 44% considered themselves as fluent, while only 8% were not fluent at all. In addition, 81% of the sample have used between 1–5 IoT devices and 51% plan to more adoption of new IoT products in the future.

4.3. Reliability and Validity

Cronbach's alpha test is commonly used to evaluate survey reliability through measuring internal consistency. It indicates the degree in which the survey's participants would respond to the same questions in the same way or closely each time. The Cronbach alpha values of each framework's dimension of factors were analyzed to consider their reliability based on the theoretical model. The values should meet the minimum accepted criteria, that is, above 0.6, in order to confirm the model consistency and reliability [29,38]. Results indicate that Cronbach's alpha values ranged between 0.74 and 0.9, which is greater than the approved threshold. This reflects a good internal consistency and reliability. Consequently, the questionnaire was considered to be composed of a set of consistent variables for capturing the meaning of the trust factors.

The overall analysis produced an excellent fit for the tested model using different validity measures. Firstly, SEM analysis using Goodness of Fit Index (GFI) was applied to assess the fit between the survey data and the model. GFI has the criteria that if its value ranges between 0.9 and 0.94, then it is an acceptable fit, and, if it is between 0.95 and 1.0, then it is a good fit. Results show that the GFI is higher than 0.9 as (0.997, 0.923 and 0.968), demonstrating a good fit between the conceptual model and the collected data. Therefore, it could be said that the suggested trust model is valid in a real environment. Table 2 presents the reliability analysis and the GFI attribute value for each construct.

Table 2. Validity and reliability analysis.

Construct	Goodness Fit Index (GFI) Value	Acceptance Analysis	Average Variance Extracted (AVE)	α Value	α Value Analysis
Product-related factors	0.997	Good Fit	0.998	0.90	Excellent
Social influence related factors	0.923	Acceptable Fit	0.959	0.76	Good
Security-related factors	0.968	Good Fit	0.843	0.74	Good

In order to test convergent validity, which is used widely in behavioral science, average variance extracted (AVE) and discriminate validity were employed. The results, presented in Table 2, show that all AVEs exceed 0.5. Accordingly, the scale has a good convergent validity. The model's discriminate validity was evaluated by examining each pair of dimensions' correlations using Spearman's rho test, which measures the Spearman's rank correlation coefficient to evaluate the degree of relationship between two variables using a monotonic function [39]. The data analysis demonstrated a positive relationship between all dimensions as stated in Table 3, and indicated the model's discriminate validity and convergent validity.

Table 3. Model correlation analysis.

Variables	Correlation Coefficient	Conclusion
Product related factors—Social influence related factors (H1–H2)	0.447	Moderate positive relationship
Product related factors—Security related factors (H1–H3)	0.56	Moderate positive relationship
Social influence related factors—Security related factors (H2–H3)	0.389	Moderate positive relationship

4.4. The Statistical Analysis

Each dimension of factors was assessed in a hierarchical manner based on the Likert scale attitude analysis to cover each element. An assessment scale of 1–5 was used to rate each response, with 5 indicating a highly influential factor and 1 representing a factor with no influence, as shown in Table 4. Then, the weight distribution calculated based on the assessment scale was applied to distinguish negative versus positive perceptions.

Table 4. Assessment Scale.

Grade	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Value	1	2	3	4	5

Each factor was then reported in weight and frequency. After that, results were accumulated in order to evaluate each dimension of factors based on their aggregated weight. Factors with poor weights were excluded as they could be considered to have little relation to or effect on consumers' decision. In contrast, highly weighted items indicated a positive relevance. Items that fell in the middle weight range were restudied to be removed or improved, as this specified that the consumers were unsure about the relevance of these factors to their decision. The statistical aggregation of responses permitted a quantitative data analysis and interpretation [40].

The average weight—represented by different statements that represent each dimension of factors—was calculated in order to determine an overall mean for each dimension. Results of the statistical analysis of the survey data are summarized in Table 5.

Table 5. Results' statistical analysis.

Factors	Mean	Frequency	Standard Error	Median	Standard Deviation	Confidence Interval
H1 Product-related factors	4.15	-	0.04	4	0.78	(4.06–4.23)
H1A IoT technology Functionality and reliability	4.1	77%	-	-	-	-
H1B IoT technology helpfulness	4.21	71%	-	-	-	-
H1C perceived ease of use	4.07	77%	-	-	-	-
H1D perceived usefulness	4.21	83%	-	-	-	-
H2 Social Influence related factors	4		0.05	4	0.97	(3.9–4.1)
H2A Consumer's social network.	4.01	78%	-	-	-	-
H2B Community interest.	3.99	68%	-	-	-	-
H3 Security of products and services related factors	4.18	-	0.05	4.6	0.94	(4.08–4.27)
H3A Product or service's security	4.28	83%	-	-	-	-
H3B perceived risk associated	3.99	74%	-	-	-	-
H0. The level of trust in the IoT technology is positively associated with the adoption of IoT	4.11	-	0.046	4.2	0.897	-

The mean of average weights of the three dimensions of factors was above 4, indicating a positive reflection and attitude. With a 95% confidence interval, the minor range (0.17, 0.2 and 0.19) confirms the acceptance of the selected factors to build consumer trust towards IoT adoption and indicates that the mean is sufficiently representative. Security of products and services related factors received the highest mean value followed by product-related factors and then social influence related factors. The mean of the factors is ranging between 3.99 and 4.21, which was in the acceptable rate. The mean value could be used to order the factors from most important to least important. The confidence interval values correspond to the mean value in terms of order, indicating a consistency in the results.

Moreover, each dimension standard deviation was close to zero (0.78, 0.97, 0.94), indicating a positive impression towards the proposed factors. The small standard deviation values indicated a small distance from the mean. Hence, the resulting mean values were considered to be good representatives of the dataset and showed precise responses; we can trust the resulted mean values. Furthermore, the least standard deviation value of product-related factors revealed the significance of this dimension to the consumer trust towards IoT adoption. A small standard error values (0.04 and 0.05) indicated that the sample means were related to the population mean; consequently, we can say that the sample is a good reflection of the population and the value of the mean is representative of the dataset.

To analyze each dimension of factors' frequency distribution, the positive perception answers were clustered together to indicate a "favorable" response. In contrast, "unfavorable" responses involved negative perception responses. This clustering enabled us to display the data in a comprehensible format. Responses show that participants received the proposed set of dimensions positively. Consequently, these dimensions were considered significant in affecting the trust and the decision of consumers towards the adoption of IoT, as more than 70% of respondents were in favor of every domain of factors. The frequency distribution of each dimension is shown in Figure 2. It indicated that the security of products and services-related factors were influential factors, with 79% favorable responses, followed by product-related factors with 72% favorable responses and then social influence-related factors with 70% favorable responses. With regards to factors, perceived usefulness received the highest favorable responses with 88% followed by product or service security with 83%. Consumer social network effect, functionality and reliability, and ease of use were next in importance to survey respondents with around 77%. These were followed by perceived risks of the products followed by product helpfulness. The least factor was the community interest with 68% favorable answers, indicating a low effect of the local community and culture on the trust decision.

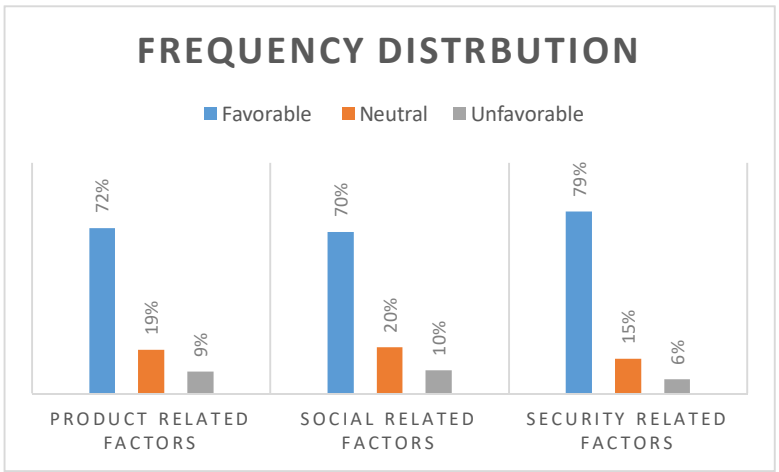

Figure 2. Frequency distribution of the framework dimensions.

5. Discussion

This study aimed to identify the factors that influence users' trust towards the adoption of IoT technologies. The results of the data analysis collected through the survey confirm the robustness of the proposed IoT technology trust model. It was revealed via statistical analysis that the three dimensions of factors and sub-factors are accepted to be influencers of trust and adoption decision. This shows that the framework structure is valid and approved. The study found that consumers' decision towards the adoption of IoT technology could be influenced by three dimensions of factors. These dimensions include product-related factors, which are related to product functionality and reliability, helpfulness, ease of use, and consumer's perceptions of usefulness. In addition, social-related factors such as social influence and community interest could also influence users' trust decision. Finally, security-related factors are influential, including product (trustee) security and consumers' perceived risks.

The dimensions of factors were evaluated using the survey. In comparing the mean and percentage of the different dimension and factors of the model, security-related factors were found to be the most influential in relation to the other factors. Moreover, product (trustee) security was perceived to be the most critical factor that affects consumers' decision to trust an IoT product. This indicates the importance of taking care of IoT product security, as people are more aware of security threats and needs in today's digitally interconnected life as [7,12] suggested. More connected devices mean further attack vectors and increased possibilities for cybercriminals to target individuals, unless security concerns are carefully addressed. Consumers fear that their sensitive information will fall into the wrong hands or be used in inappropriate ways. Thus, IoT service and product providers should address these security concerns by providing appropriate security controls such as Public Key Infrastructure (PKI), encryption, transparency to enhance data security, and best practices in data management. The industry needs to demonstrate that consumer's data is safe and treated properly in order to gain their trust.

On the other hand, respondents were less concerned about to perceived risks (74% favorable responses), in contrast to the suggestion of Khan et al. [2]. This is perhaps related to the fact that people think that assessing risks realistically is not easy, as they need to recognize, differentiate, and then assess risk. However, humans have a tendency to assume that bad things happen to others but not to them [41], especially as the majority of respondents were less than 40 years old and younger generations have usually been found to trust technology more instinctively. IoT products and service providers should build trust through high standards of physical safety to minimize the perceived risks of using these products. They also need to endorse compliance with security standards and laws as well as data privacy and protection acts.

The second dimension of factors, with a very small difference, is the product-related factors. Among this dimension of factors, the respondents ordered the factors according to the analysis, based on their importance. Perceived usefulness was the most influential factor, followed by helpfulness, product functionality and reliability, and ease of use. Perceived usefulness received the highest favorable responses among this dimension and the second among all sub-dimensions. This supports the prior research finding of Gao and Bai [11] and Koien [12], who reported that usefulness is the primary determinant of consumers' decision towards technology use. Therefore, it is very important for IoT technology providers to advocate and ensure that the product or service is useful for the end-users. Moreover, according to the mean value, helpfulness was also perceived to be an influencing factor. This indicates the importance of providing a clear, easy, and supportive help system. This could be justified as people with emerging new technologies everyday are challenged to adapt and learn how to use it and solve problems that may arise. Therefore, having a good supportive system could enhance their trust towards that technology product.

Moreover, to guarantee consumer trust, IoT products and services should act as expected, even in a hostile environment [12]. This was confirmed by the finding of the survey, as functionality and reliability were viewed by the respondents positively as influencing factors. Unexpectedly, it was found that perceived ease of use was the least influencing factor, according to the mean value, which

contradicts the findings of Gao and Bai [11]. Nonetheless, it still received as high mean value of 4.07, indicating its positive influence. Therefore, it is necessary to provide a well-designed, easy-to-use interface to end-users as a way to increase their trust of the product and make them feel more comfortable adopting it.

The social-related factors had the least effect among the three dimensions on the trust intention, with a mean value of 4.0. The majority of participants in this study were below the age of 40 years, which is an age group usually considered to be more susceptible to social influence and the new trends. As a result, the, influence of their social network can affect their decision to adopt IoT technology [11]. Seventy-eight percent of the survey respondents indicated a favorable response to the effect of their social network on their trust decision. Positive and encouraging reviews from an individual's social network might create a positive word-of-mouth influence on succeeding adoption decisions, as suggested by Choi and Lee [33]. Thus, IoT technology providers should make use of this to promote the adoption of new IoT products and services by publicizing such testimonials and obtaining celebrity endorsements, as suggested by Gao and Bai [11]. However, they are less susceptible, as the data analysis reveals, to the community interest and culture values. This contradicts the suggestion of Kowshalya and Valarmathi [34], in which community interest was identified as a significant factor that empowers trust. In brief, IoT technology providers must consider the social-related factors in order to increase consumers' trust to encourage the adoption of IoT technology.

Furthermore, the findings revealed that trust is necessary for the adoption of IoT technology but may be not a sufficient condition. To clarify, if a consumer has a low level of trust in an IoT product or service, they may not adopt it as they may consider it as un-trustworthy. However, based on the findings, trust alone or lack of trust does not inevitably lead to the adoption of IoT technology or lack thereof.

6. Conclusions and Future Work

Trust has been acknowledged as a crucial motivational factor for technology adoption [20] . In IoT, trust is important because it can deal with two critical IoT technology conditions: the threats of vulnerability and uncertainty. Furthermore, it has been proven that the success of IoT adoption positively depends upon the consumer level of trust [2]. In order to improve consumer trust toward the adoption of IoT technology, an appreciation of trust-related factors is required. From a theoretical perspective, this relationship is complex due to the dynamic nature of IoT environments [12], limited IoT resources, and the cost of security requirements. In this paper, an IoT technology trust model was proposed to cover a varied set of factors related to consumer trust that affects the decision to adopt IoT technology, including three main dimensions and eight domains. The three dimensions are: security of products and services-related factors, product-related factors, and social influence-related factors. The factors were covered in a structured way using the TAM and the social-psychological perspective to achieve a comprehensive view based on previous research.

The IoT technology trust model was evaluated through a structured survey, and data were collected from consumers who have used IoT to collect their views regarding the factors that influence their trust towards IoT technology in order to validate the proposed model. The data were statistically analyzed to confirm the results by using a suitable variable analysis technique. The main goal of this step was to measure and understand the relationships among the different related factors and variables.

According to the survey analysis, IoT products and services security and privacy are amongst the highest priorities to ensure consumers' trust, yet they still remain a challenge in IoT technology. Next, the product should appear useful to consumers with clear benefits, capabilities, and functionalities that focus on the consumer experience to boost the consumer trust to adopt IoT and boost the market. Furthermore, to achieve trust in IoT technology, it must be reliable and trustworthy, fulfill standards, and conform to some user expectations and requirements. Overall, to guarantee consumer trust in IoT products and services, product functionality and reliability, even in a hostile environment, is important. Finally, social-related factors, such as user network, were found to influence consumers'

trust decisions to adopt an IoT device. Nevertheless, community interest and local culture were the least influential factors.

This study contributes to research and practice in two ways. First, it offers a literature review to investigate the role of trust in IoT technology adoption. Second, it provides a conceptual model that gathers from the literature the factors that influence consumers' trust decisions towards IoT adoption. This model may be used by researchers to further investigate trust issues and create a trustworthy literature in the field of IoT trust. Moreover, this model could be used by IoT technology developers as a guide to the most influencing factors—from the consumers' point of view—that could enhance their trust decision towards IoT products, thus creating value for IoT technology consumers and providers.

Future work may consider specific domains of IoT products or services. This might involve adding further factors or requiring some changes to be made to the subdomains. Moreover, the model could be enhanced with practical standards and performance indicators for improving trust in IoT products and services. Furthermore, this study explored the factors influencing consumer adoption of IoT technology in one community. However, there may be some variance in cultural beliefs or governmental regulations in comparison with other communities. Thus, to verify the validity of the suggested model presented in this study, further research should expand the boundaries of investigation to other communities.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. 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]
2. Khan, W.; Aalsalem, M.; Quratulain, A.; Khan, M. Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model. In *Advanced Multimedia and Ubiquitous Engineering*; Springer: Singapore, 2016; Volume 354, pp. 479–485.
3. Del Giudice, M. Discovering the Internet of Things (IoT) within the business process management. *Bus. Process Manag. J.* **2016**, *22*, 263–270. [CrossRef]
4. Weber, R.H. Internet of Things—New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
5. Daubert, J.; Wiesmaier, A.; Kikiras, P. A view on privacy & trust in IoT. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2665–2670.
6. Yildirima, H.; Ali-Eldina, A. A model for predicting user intention to use wearable IoT devices at theworkplace. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, in press.
7. Falcone, R.; Sapienza, A. On the Users' Acceptance of IoT Systems: A Theoretical Approach. *Infomation* **2018**, *9*, 53. [CrossRef]
8. Lin, Z.; Dong, L. Clarifying Trust in Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 234–248. [CrossRef]
9. Al-Momani, A.; Mahmoud, M.; Ahmad, S. Modeling the adoption of internet of things services: A conceptual framework. *Int. J. Appl. Res.* **2016**, *2*, 361–367.
10. Belanche, D.; Casaló, L.V.; Flavián, C. Integrating trust and personal values into the technology acceptance model: The case of e-government services adoption. *Cuad. Econ. Dir. Empres.* **2012**, *15*, 192–204. [CrossRef]
11. Gao, L.; Bai, X. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pac. J. Mark. Logist.* **2014**, *26*, 211–231. [CrossRef]
12. Koien, G.M. Reflections on trust in devices: An informal survey of human trust in an Internet-of-Things context. *Wirel. Pers. Commun.* **2011**, *61*, 495–510. [CrossRef]
13. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context Aware Computing for The Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 414–454. [CrossRef]
14. Farooq, M.U.; Waseem, M.; Khairi, A.; Mazhar, S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6.

15. Yan, Z.; Zhang, P.; Vasilako, A. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
16. Report, T.D.T. 2018 Global Data Threat Report. *Thales Data Threat Report*. 2018. Available online: https://dtr.thalesesecurity.com/ (accessed on 23 June 2018).
17. McKnight, D.; Carter, M.; Thatcher, J.; Clay, P. Trust in a specific technology: An investigation of its components and measures. *ACM Trans. Manag. Inf. Syst.* **2011**, *2*, 12. [CrossRef]
18. Mayer, R.; Davis, J.; Schoorman, F. An integrative model of organizational trust. *Acad. Manag. Rev.* **1995**, *20*, 709–734. [CrossRef]
19. Tam, S.; Thatcherb, J.B.; Craigc, K. How and why trust matters in post-adoptive usage: The mediating roles of internal and external self-efficacy. *J. Strateg. Inf. Syst.* **2017**, *27*, 170–190.
20. Gefen, D.; Karahanna, E.; Straub, D. Trust and TAM in online shopping: An integrated model. *MIS Q.* **2003**, *27*, 51–90. [CrossRef]
21. Han, B.; Wu, Y.A.; Windsor, J. User's Adoption of Free Third-Party Security Apps. *J. Comput. Inf. Syst.* **2014**, *54*, 77–86.
22. Renaud, K.; van Biljon, J. Predicting technology acceptance and adoption by the elderly. In Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries Riding the Wave of Technology—SAICSIT'08, Wilderness, South Africa, 6–8 October 2008; pp. 210–219.
23. Coughlan, T.; Brown, M.; Mortier, R.; Houghton, R.; Goulden, M.; Lawson, G. Exploring Acceptance and Consequences of the Internet of Things in the Home. In Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Besancon, France, 20–23 November 2012; pp. 148–155.
24. Khan, M.K. Building Consumer Trust in Adopting IoT Enabled Products. In Proceedings of the International Conference for Information and Network Security, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 2–3 May 2017.
25. Thatcher, J.B.; McKnight, D.H.; Baker, E.W.; Arsal, R.E.; Roberts, N. The role of trust in postadoption IT exploration: An empirical examination of knowledge management systems. *IEEE Trans. Eng. Manag.* **2011**, *58*, 56–70. [CrossRef]
26. Lee, M.; Turban, E. A Trust Model for Consumer Internet Shopping. *Int. J. Electron. Commer.* **2001**, *6*, 75–91. [CrossRef]
27. Chang, S.-H.; Chou, C.-H.; Yang, J.-M. The Literature Review of Technology Acceptance Model: A Study of the Bibliometric Distributions. *Pac. Asia Conf. Inf. Syst.* **2010**, *158*, 1634–1640.
28. Cho, Y.C.; Sagynov, E. Exploring Factors that Affect Usefulness, Ease of Use, Trust, and Purchase Intention in the Online Environment. *Int. J. Manag. Inf. Syst.* **2015**, *19*, 21–35. [CrossRef]
29. Lai, I.K.W.; Tong, V.W.L.; Lai, D.C.F. Trust factors influencing the adoption of internet-based interorganizational systems. *Electron. Commer. Res. Appl.* **2011**, *10*, 85–93. [CrossRef]
30. Bart, Y.; Shankar, V.; Sultan, F.; Urban, G.L. Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *J. Mark.* **2005**, *69*, 133–152. [CrossRef]
31. Hochleitner, C.; Graf, C.; Unger, D.; Tscheligi, M. Making Devices Trustworthy: Security and Trust Feedback in the Internet of Things. In Proceedings of the Pervasive'12 Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK, 18–22 June 2012.
32. Abu, F.; Jabar, J.; Yunus, A.R. Modified of UTAUT Theory in Adoption of Technology for Malaysia Small Medium Enterprises (SMEs) in Food Industry. *Aust. J. Basic Appl. Sci.* **2015**, *9*, 104–109.
33. Choi, B.; Lee, I. Trust in open versus closed social media: The relative influence of user- and marketer-generated content in social network services on customer trust. *Telemat. Inform.* **2017**, *34*, 550–559. [CrossRef]
34. Kowshalya, A.M.; Valarmathi, M.L. Trust management for reliable decision making among social objects in the Social Internet of Things. *IET Netw.* **2017**, *6*, 75–80. [CrossRef]
35. Blomqvist, K.; Hurmelinna-Laukkanen, P.; Nummela, N.; Saarenketo, S. The role of trust and contracts in the internationalization of technology-intensive Born Globals. *J. Eng. Technol. Manag.* **2008**, *25*, 123–135. [CrossRef]

36. Pak, R.; Rovira, E.; McLaughlin, A.; Baldwin, N. Does the domain of technology impact user trust? Investigating trust in automation across different consumer-oriented domains in young adults, military, and older adults. *Theor. Issues Ergon. Sci.* **2016**, *18*, 199–220. [CrossRef]
37. Chen, L.; Yan, Z.; Zhang, W.; Kantola, R. TruSMS: A trustworthy SMS spam control system based on trust management. *Future Gener. Comput. Syst.* **2015**, *49*, 77–93. [CrossRef]
38. AlHogail, A. Cultivating and Assessing Organizational Information Security Culture, an Empirical Study. *Int. J. Secur. Appl.* **2015**, *9*, 163–178.
39. Pallant, J. *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using SPSS for Windows*; Open University Press: Berkshire, UK, 2010.
40. Skulmoski, G.; Hartman, F. The Delphi Method for Graduate Research. *J. Inf. Technol. Educ.* **2007**, *6*, 1–21. [CrossRef]
41. West, R. The psychology of security: Why do good users make bad decisions? *Commun. ACM* **2008**, *51*, 34–40. [CrossRef]