Journal of International Technology and Information Management

Manuscript 1572

An Empirical Study to Understand the Role of Institution-Based Trust and Its Antecedents in IoT Adoption by Individuals

Anupam Kumar Nath

Amit Kumar Nath

An Empirical Study to Understand the Role of Institution-Based Trust and Its Antecedents in IoT Adoption by Individuals

Anupam Kumar Nath
(*Georgia Gwinnett College*)

Amit Kumar Nath
(*Florida State University*)

ABSTRACT

The Internet of Things (IoT) enables the connection between humans, physical objects, and cyber objects, resulting in monitoring, automation, and decision-making capabilities. This connection can be complex and lead to uncertainty for individuals before adopting IoT technology. To address this, we conducted research on the role of Institution-based trust in the context of IoT adoption. Our model for IoT adoption is based on existing literature and includes the components of Institution-based trust and its antecedents. Through empirical testing, we confirmed that Institution-based trust positively affects IoT adoption at the individual level. Additionally, we found that User confirmation/disconfirmation and familiarity are the antecedents of Institution-based trust.

Keywords: Internet of Things (IoT), Trust, Technology Adoption, Institution based trust

INTRODUCTION

The current trend to interconnect various kinds of devices and systems has produced the increasingly popular paradigm of the "Internet of Things (IoT)." IoT has brought several benefits to users through increased control, remote management, and volume of available usage information (Atzori & Morabito, 2010). Homes are converted to "smart" through the integration of IoT technology in various home activities. With numerous benefits due to increased information and control, the technology also introduced various vulnerabilities to allow remote management and communication between devices (Wendzel et al. 2014). These vulnerabilities have raised privacy, security, and overall trust concerns (AlHogail,2018; Menard & Bott, 2018). This is a similar scenario that occurred with the emergence of e-Commerce a few decades ago and then for M-commerce (Giovannini et al., 2015). Similarly, trust should play a key role in the successful adoption of IoT (Nord et al.,2019; Falcone& Sapienza,2018; Khan et al.,2016). Institution-based trust played a vital role in understanding users' perceived trust in the E-commerce environment (McKnight et al., 1998). Furthermore, institution-based trust helps individuals operate in an unfamiliar environment (Zucker, 1986). Hence, we can infer that Institution-based trust will play a role in the adoption of a relatively newer technology like IoT. We also wanted to identify factors affecting the user's institution-based trust. Consequently, the following two research questions guide this research:

RQ1: What role does institution-based trust play in the adoption of IoT devices by individuals?

RQ2: What are the factors that affect an individual's Institution-based trust in IoT adoption?

This research aims to develop a theoretical model to comprehensively understand the role of Institution-based Trust in the context of the IoT environment. Previous studies have highlighted the significance of institution-based trust in two dimensions: structural assurance and situational normality (McKnight et al., 1998). Building on this knowledge, our proposed model identifies three fundamental elements of Institution-based Trust in the context of IoT: Perceived IoT device quality, Perceived IoT device effectiveness, and Perceived Trustworthiness of IoT. By incorporating these elements, our theoretical model allows us to delve deeper into the role of trust in the IoT environment. Our model also outlines the antecedents of Institution-based trust at the personal level. We believe that understanding the factors that influence trust at an individual level is crucial to comprehend the adoption and use of IoT devices. Hence, we have conducted an empirical evaluation

.

of the proposed model. Our evaluation demonstrates the importance of institution-based trust and its antecedents in adopting IoT devices at the individual level. Our findings make a significant contribution to the literature on emerging technology adoption and trust. Our theoretical model and empirical evaluation provide a foundation for comprehensively understanding the role of trust in the IoT environment and how it influences the adoption and use of IoT devices.

The following section gives an overview of the existing literature on trust's role in IoT adoption at the individual level. We then outline our conceptual model and develop our hypotheses. The next section describes the data collection, method, and analysis strategy. The following section presents the results and the discussion on the results. We conclude the paper with practical implications of our findings and suggestions for future research.

LITERATURE REVIEW

The Internet of Things (IoT) has become an exploration focus for both industry and academia. The features and capabilities that the IoT offers are the main motivations for gaining significant attention in both fields. It is also related to several human-related factors (Perera et al., 2014). Trust is one such human factor. We conducted a literature review to identify studies that examined trust as a factor in the adoption of IoT devices. Our primary focus was on business literature, but we also included other studies that investigated trust as a factor in individual's adoption of IoT devices. Trust is one's willingness to place oneself in a vulnerable position (Mayer et al., 1995) and the expectation that others one chooses to trust will not behave opportunistically by taking advantage of the situation (Gefen et al., 2003). Whenever a new technology emerges that involves sharing information, it has historically raised concerns about security and privacy. (Nord et al.,2019; Voas et al., 2018). In extant literature, trust played a vital role in addressing those concerns (Jasper & Pearson, 2022; Al-Momani et al., 2016; Giovannini et al., 2015). Researchers are now exploring the significance of trust in the IoT environment. However, most studies have focused on the technical aspects of "Trust" rather than the consumer's perspective. Aldossari & Sidorova (2018) is one of the few papers that have studied trust from a consumer's perspective. The paper draws upon the unified theory of acceptance and use of technology and finds that trust and security risk play a vital role in accepting IoT. In 2018, Alhogali proposed a conceptual model aimed at enhancing the adoption of IoT. The model incorporates consumer trust as one of its constructs. Pal et al. (2019) studied trust as one of the factors in the continuance intention to use wearable IoT devices. Alraja et al. (2019) studied

.

and found the importance of trust in the context of IoT-based healthcare. Lee (2019) studied the trust's role in users' perceived security risk in the IoT environment. Esmaeilpour et al. (2020) developed a model to analyze how the Internet of Things (IoT) contributes to the growth of e-business. Their model highlights the crucial role of trust in this process. More recently, Jasper & Pearson (2022) studied perceived usefulness, trust, and privacy concerns as drivers of adoption of the domestic IoT devices. The study found the significance of trust and perceived usefulness in IoT adoption. While these studies highlight the importance of studying trust in the IoT environment, the existing research also indicates a requirement for additional studies based on empirical evidence regarding the significance of trust in institutions for consumers' adoption of IoT.

THEORY DEVELOPMENT

Trust

Different disciplines examined trust as a construct, including but not limited to management, psychology, sociology (Yuliati et al., 2020; Khan et al., 2015; Beldad et al., 2010; Butler, 1991; Corazzini, 1977; Lewis and Weigert, 1985; McKnight et al.2002; McKnight and Chervany, 2000; Muir, 1994). Formally, the overall trust concept means a secure willingness to depend on a trustee because of that trustee's perceived characteristics (Karale, 2021; Khan et al., 2015; Rousseau et al., 1998). Three major types of applicable trust concepts are used: trusting beliefs, trusting intentions, and trusting behaviors. These concepts are connected. Trusting beliefs means a secure conviction that the other party has favorable attributes such as benevolence, integrity, and competence. Trusting intentions means a secure, committed willingness to depend upon, or to become vulnerable to, the other party in specific ways, strong enough to create trusting behaviors. Trusting behaviors mean assured actions that demonstrate that one depends or relies upon the other party instead of on oneself or controls. Trusting behavior is the action manifestation of willingness to depend. Each of these generic trust types can be applied to trust in IT. Trusting behavior-IT means that one securely depends or relies on technology instead of trying to control the technology.

Based on the offline expectation-based trust as a starting point, researchers have elaborated upon one another's definitions and emphasized online environments' specific characteristics to form online trust definitions. Trust plays a vital role in IoT for reliable data fusion and mining, qualified services with context awareness, and enhanced user privacy and information security (Aaqib et al., 2023). Trust becomes even more critical when users share personal information with service

.

providers. Home IoT service providers, through the myriad of IoT devices, can collect and store personal information in the real world, and they can access to detailed behaviors of the user (Aaqib et al., 2023).

Researchers made efforts to provide consistent measures for trust in the online context that builds upon a solid and theoretical foundation and that have been validated through empirical analysis (McKnight et al., 2002; Pavlou & Gefen, 2004). From E-commerce to trust has been extended to the M-commerce domain (Giovannini et al., 2015). As the next logical progression, we extend the trust concept, specifically institution-based trust, to the domain of a newer phenomenon-IoT.

Figure 1 illustrates our proposed theoretical model and the relevant relationships for our study. The subsequent sections will provide a comprehensive overview of this model.

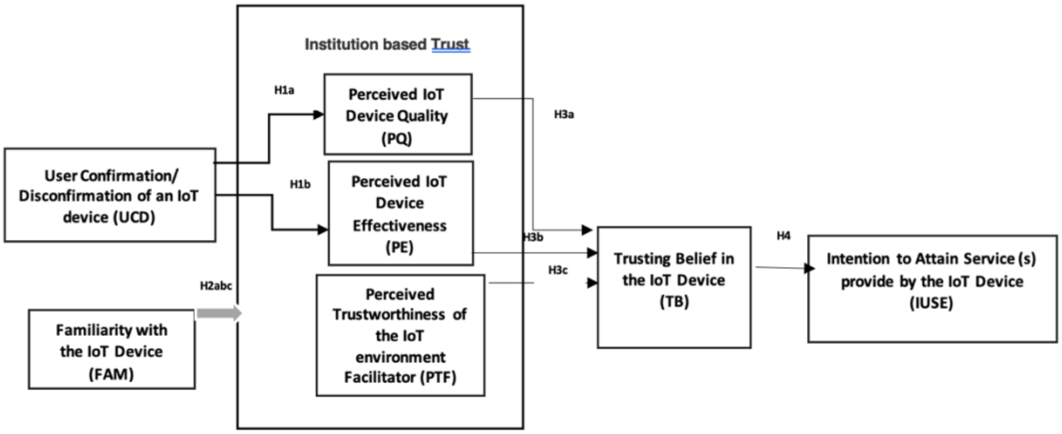
Institution based Trust
H1a
Perceived IoT Device Quality (PQ)
H3a
User Confirmation/ Disconfirmation of an IoT device (UCD)
H1b
Perceived IoT Device Effectiveness (PE)
H3b
H4
Trusting Belief in the IoT Device (TB)
Intention to Attain Service (s) provide by the IoT Device (IUSE)
H3c
H2abc
Familiarity with the IoT Device (FAM)
Perceived Trustworthiness of the IoT environment Facilitator (PTF)

Figure 1. Proposed Theoretical Model

Institution-based Trust

Institution-based trust helps individuals operate within an impersonal and unfamiliar environment. (Yuliati et al., 2020; Shao & Yin,2019; Zucker, 1986). There are two dimensions of institution-based trust: structural assurance and situational normality (Loeonard & Jones, 2021; McKnight et al., 2011; McKnight et al., 1998). Structural assurance posits that the presence of institutions such as rules and regulations that promote safety and security will increase trust in an environment wherein people are unknown to one another. Situational normality

.

suggests that an environment that is in proper order is conducive to trust, and therefore, successful interaction is possible within that kind of environment. Due to the importance of trust in the Internet's impersonal environment, structural assurance and situational normality in institution-based trust have been adapted toward investigations of trust within the e-commerce context. Institution-based trust is a key component of successful e-commerce transactions and also the consumer's assumptions of legal and regulatory protections are integral to trust formation Tandon et al., 2021; Yuliati,at al., 2020; Shao & Yin,2019; McKnight and Chervany, 2002). Ratnasingam and Pavlou (2002) describe structural institution-based trust in the context of B2B e-commerce as technology trust, which encompasses trust engendered via the presence of technical standards, security, and other protective mechanisms. Internet's structural characteristics, such as technical and safety mechanisms, positively influences trusting beliefs in the online context (Loeonard & Jones, 2021). In applying the concept of situational normality to the Internet environment, McKnight et al. (2002) suggest that situational normality is high when the consumer perceives the environment as in good order, and vendors in the environment are competent, benevolent, and have integrity. Here competent means possessing the capability to do a task or fulfill a responsibility, benevolent means morally sound, and integrity means having truthfulness and honesty.

Following Pavlou (2002,2003), who suggests there is a need to design institution-based trust in specific contexts, we have incorporated three specific components of institution-based trust in the context of IoT environment: Perceived IoT Device Quality, Perceived IoT device Effectiveness, Perceived Trustworthiness of the IoT Facilitator.

User Confirmation/Disconfirmation of an IoT Device

Expectation Confirmation Theory (ECT) posits that satisfaction depends on the extent to which consumers perceive their initial expectations of services to be confirmed or disconfirmed during actual use (Fan & Suh, 2014; Oliver, 1980) and has been validated across information systems use behaviors (Ha et al., 2021; Bhattacharjee,2001). In the e-commerce context, ECT expectations refer to consumers' beliefs about the potential utility that can be derived from an e-commerce-based service (Wang et al., 2020). Expectation forms the baseline against which users will form judgments about an IoT device. In the context of institution-based trust in the current study, a user will have expectations of the IoT device's effectiveness and quality that will be confirmed or disconfirmed during actual use. In this study, we suggest that when a user confirms or disconfirms an IoT device, it will positively impact their perception of the system's quality and effectiveness.

.

Hypothesis 1a (H1a). A user's confirmation/disconfirmation of an IoT device positively influences perceived IoT device quality.

Hypothesis 1b (H1b). A user's confirmation/disconfirmation of an IoT device positively influences perceived IoT device effectiveness.

Familiarity with an IoT Device

In the early days of e-commerce, individuals familiar with a website had a better understanding of its content, layout, and navigation than those unfamiliar with it. (Agarwal and Venkatesh, 2002). Such "situational normality" (McKnight et al., 2002). can be extended towards IoT devices. The underlying assumption is that, generally, having knowledge about IoT devices will enhance a person's trust in them. This is because the person will view their interaction with the devices as appropriate and ordinary. (Alraja & Faooque,2019; Malkin at al., 2019)). We can apply the theoretical aspect of Task Complexity, which suggests that familiarity with IoT devices is a factor that will positively influence institution-based trust. Studies using task complexity theory (e.g., Agarwal and Venkatesh, 2002; Cox & Cox, 2002) have supported the conclusion that the user who is familiar with a particular website has clearer and better understanding of the content, organization, and browsing procedures of the website than individuals who are unfamiliar with the web. Accordingly, a consumer comfortable with the Web situation is likely to have high trusting beliefs in a specific vendor in general (McKnight et al., 2002). Following the same justification, our research model suggests that familiarity with IoT devices will have a direct and positive relationship with institution-based trust (Alraja & Faooque,2019). Consequently, a user's familiarity with IoT devices indirectly influences trusting beliefs through each component that makes up institution-based trust.

Hypothesis 2a (H2a). A user's familiarity with an IoT device positively influences perceived IoT device quality.

Hypothesis 2b (H2b). A user's familiarity with an IoT device positively influences perceived IoT device effectiveness.

Hypothesis 2c (H2c). A user's familiarity with an IoT device positively influences the perceived Trustworthiness IoT environment facilitator.

.

Perceived IoT device Quality

In the initial phase of trust development, initial trust forms quickly based on 'whatever information is available' (AlHogail ,2018; Meyerson et al., 1996). This 'information available' often comes in the form of small signals or cues that a party is trustworthy (Menon et al., 1999). McKnight et al. (2002) suggest that people make trust-related assumptions on the web, where the other party is mostly "faceless" based on their perception. Perceptions depend on aspects like the perceived build quality of the web front, user-friendly interface, and resemblance with other well-reputed entities. Then in a similar "Faceless" situation of conversional agent, perceived quality of the technology plays a role in building trust (Rheu et al., 2021). We can extend this "perceived quality" construct to the IoT environment where a user interacts with the service facilitator and provider through IoT devices. Therefore, we hypothesize that the user's perception of IoT device quality will impact his or her perceptions of the service provided by the system. Thus, a user will be more likely to view a service as trustworthy if it derives from an IoT device perceived as high quality. Therefore, we hypothesize that the users' perception of IoT device quality will positively impact the user's trusting belief in IoT device(s).

Hypothesis 3a(H3a). A user's perception of an IoT device's quality will positively influence trusting beliefs in an IoT device.

Perceived IoT device Effectiveness

User's perception of institutional mechanisms' effectiveness is essential in online environment (Sim et al., 2018; Kim et al., 2009). In the context of this study, in accordance with Pavlou and Gefen (2004), we describe effectiveness based on two aspects. Two factors judge the effectiveness of an IoT device. Firstly, how reliable, helpful, and dependable the user perceives the device's mechanisms. Secondly, whether the user believes enforceable and cost-effective mechanisms are in place to resolve disputes or problems. In essence, a user's perception of an IoT device's effectiveness directly affects their perception of its service quality. Hence, we hypothesize that as users' perception of an IoT device's effectiveness increases, so will their trusting beliefs about that IoT device.

Hypothesis 3b (H3b). A user's perception of an IoT device's effectiveness will positively influence trusting beliefs in an IoT device.

.

Perceived Trustworthiness of IoT Facilitator

Extant research found that trust transference can occur intra-channel when trust is transferred from one entity to another in the same channel (Ballester & Espallardo, 2008; Stewart, 2003, 2006). It can also happen inter-channel when trust is transferred from one context to another (Hahn & Kim, 2009; Kuan & Bock, 2007; Lin et al., 2011). For example, Lin et al. (2011) found that trust in online brokerage services directly affects initial trust in mobile brokerage services. Therefore, we infer that users' trust in a company's current web-based and mobile-based services will transfer to the IoT environment when they serve as IoT facilitators. Pavlou and Gefen (2004) and McKnight and Chervany (2000) suggest that unknown parties often draw trust in the online context through their association with a trusted entity. Therefore, we hypothesize that users will draw trust-related conclusions about an IoT device because they trust the IoT environment facilitator.

Hypothesis 3c (H3c). A user's perception of an IoT environment facilitator's trustworthiness will positively influence trusting beliefs in an IoT device.

Trusting Beliefs in the IoT Device and Intention to Use Service from an IoT Device

Based on the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1980), we can conjecture that trusting beliefs lead to trusting intentions. McKnight et al. (1998) recognized trusting intentions concerning consumer trust in terms of behavioral intention. McKnight et al. (2002) have extended subjective measures of trusting intention specifically for the e-commerce domain. These measures are not yet evaluated in the context of the Intention to Attain service (s) provided by the IoT Devices. We extend the measures for this relatively newer extension of e-commerce-IoT. The proposed measures are as follows: provide the IoT device personal information, engage in an interaction, and act on IoT provided service or information. `

Kim and Benbasat (2006) have identified trusting belief as an important mediator leading to trusting intentions in studies of trust in e-transactions. McKnight and Chervany (2002) have broadly defined trusting beliefs as meaning that "one believes that the other party has one or more characteristics beneficial to oneself" (p. 46). In general, trusting beliefs can be defined as the trustor's perception that the trustee shows attributes such as those beneficial to the trustor. McKnight et al. (2002) have described trusting belief as competence, benevolence, and integrity in the context of e-commerce and a web vendor.

.

In e-commerce studies (e.g., Kim and Benbasat, 2006; Lim et al., 2006; Stewart, 2006), three characteristics are commonly used to evaluate vendors: competence, benevolence, and integrity. Competence refers to the vendor's ability to successfully complete transactions, while benevolence refers to the vendor's customer care and commitment to acting in their best interests. Lastly, integrity reflects the vendor's honesty in keeping their commitments. These traits have been applied broadly across various studies. Hence, we can extend and apply them towards trusting beliefs in IoT devices (Thapa et al., 2023; Mari & Algesheimer ,2021). We hypothesize that increased Trusting Beliefs in IoT devices' services will lead to increased Intention to Attain service (s) provided by the IoT device.

Hypothesis 4 (H4): A user's trusting beliefs in an IoT device positively influences intention to attain service from an IoT device.

.

RESEARCH METHODOLOGY

Operationalization of Theoretical Model

Measurement Instrument

We developed measurement instruments for this study. All measurement items were based on existing items and measured using 1=strongly disagree, 4=neutral, and 7=strongly agree Likert-type scales. We took standard precautions to ensure the appropriateness of the measurement instrument, including a panel review and a pilot test using a sample of 121 respondents (Kim et al., 2007; Moore and Benbasat, 1991). The survey was reviewed by four information systems experts, including professors and professionals, to ensure its content validity before sharing it with the pilot study participants. After receiving their feedback, we made necessary wording adjustments to improve the survey's content and clarity.

Data Analysis Method

Partial least squares (PLS) (Hair, 2017; Chin, 1998; Wold, 1975) was used as the data analysis method this study.   PLS, an alternative to covariance-based methods (Haenlein and Kaplan, 2004), focuses on maximizing the variance of the dependent variables explained by the independent variables instead of reproducing the empirical covariance matrix. The PLS technique has become a widely used alternative to the covariance-based SEM technique and can either be applied for theory confirmation or theory development (Chin, 1998; Chin and Todd, 1995),

.

and has been applied across a wide range of studies in the information systems literature (Jaspers & Pearson, 2022; Hwang, 2005; Karimi, Somers and Gupta, 2004; Pavlou and Dimoka, 2006; Rivard and Huff, 1988; Wixom and Watson, 2001), among others. SmartPLS with the bootstrap re-sampling method (one hundred re-samples) was used to test the measurement and structural models.

To evaluate the measurement models' internal consistency, convergent validity and discriminant validity were tested (Hair, 2017). We evaluated internal consistency on pilot study by calculating composite reliability and Cronbach's alpha (Fornell and Larcker, 1981). Composite reliability and Cronbach's alpha scores should be greater than the benchmark of 0.70 (Fornell and Larcker, 1981). Each composite reliability value was well above 0.70, indicating adequate internal consistency (Nunnally, 1978). Convergent and discriminant validity can be verified when the square root of the construct's AVE is larger than the correlations with other constructs (Chen et al., 1997), loadings on that hypothesized construct are greater than 0.50, and the items for each construct load onto one factor with an eigenvalue greater than 1.0 (Wixom and Watson, 2001). We also verified convergent and discriminant reliability and the items for each construct did load onto one factor with loadings greater than 0.50, and with an eigenvalue greater than 1.0, validating and verifying the measurement properties of the constructs inherent in our theoretical model.

Participants and Positioning of Study

The study involved voluntary participation of 295 students, both graduate, and undergraduate, from two universities located in the United States. The majority of the participants were pursuing a degree in business. The researchers chose students as participants because they have been shown to exhibit similar online behavior patterns as non-students, making them a good representative of people's general behavior in the online environment. According to Ahuja et al. (2003), this approach helps to ensure that the study's findings are generalizable to the broader population.

Of the participants, more than 85% reported that they had been using IoT devices for at least one year, indicating that they had some experience with IoT technology. Additionally, the average internet experience of the participants was found to be more than ten years, which suggests that they are well-versed in using the internet. The researchers have provided further details on the characteristics of the study participants in Table 1, which includes information such as participant gender, age, and experience with different types of IoT devices.

.

The study aimed to collect data on factors related to the adoption, intention to use, and trust of IoT devices. To achieve this, the data were gathered using a web-based survey tool that underwent testing with a preliminary group of 100 respondents before being distributed to participants. The survey tool had a quality check that eliminated respondents who finished the survey too quickly (less than 33% of the median completion time), those who gave pattern responses, and those who provided straight-line answers. Moreover, the survey tool ensured that only human respondents could take the survey. This was achieved by keeping robots out of the survey. In exchange for their participation in the survey, respondents received a class credit. On average, it took respondents slightly less than five minutes to complete the survey. The survey questions were carefully crafted to ensure that they were clear, concise, and relevant to the topic at hand. At the beginning of the survey, respondents gave their consent to participate. They were then asked an initial question to determine whether they owned any IoT devices. Following this, the survey asked respondents about various factors related to IoT adoption, such as their experience with IoT devices, their intention to use these devices in the future, and their trust in them. Overall, the study aimed to collect reliable and detailed data on factors related to the adoption, intention to use, and trust of IoT devices, and the survey tool was designed to ensure that the collected data were of high quality.

.

Table 1. Study Demographics

Measure	Value	Percentage
Gender	Male	58.6%
	Female	42.4%
Age	18-25	74.8%
	26-35	17.4%
	36-55	6.9%
	>55	0.9%
Degree Studying	Business	87.2%
	Non-Business	12.8%
Income Level	<$20,000	66.4%
	$20,000--$40,000	21.6%
	$40,001--$60,000	5.0%
	$60,001--$80,000	2.7%
	$80,000>	4.3%

Results

As part of our study on IoT devices and the environment, we requested participants to complete a survey. We obtained a total of 325 responses. After careful review, we removed responses that were incomplete or had invalid data. This left us with 295 valid responses.

Measurement Models

We calculated measurement model based on the collected usable data. The following tables provide the reliability scores and correlation matrices for the reputation systems used in our study, with the square roots of AVEs for each construct reported on the diagonal.

As noted in Tables 2 and 3, Cronbach’s alpha and composite reliability scores are well above their respective standard minimum thresholds, except for the alpha score for PTM, which is slightly below the minimum threshold of .70. However, while Cronbach's alpha is often used to assess internal consistency, it implicitly assumes

.

that each item carries the same weight. Composite reliability, on the other hand, relies on the actual loadings to construct the factor score and is thus a better measure of internal consistency (Fornell and Larcker, 1981). In each case, composite reliability is well above the minimum threshold of .70 (Chin, 1998; Hulland, 1999). Additionally, the square roots of the constructs' AVEs are larger than the correlations with other constructs. Thus, the measurement models are validated and verified for the measurement properties of the constructs inherent in our theoretical model.

Table 2. Reliability

Construct	**Composite Reliability**	**Cronbach's Alpha**
PE	0.82	0.74
FAM	0.90	0.76
IUSE	0.95	0.94
PQ	0.87	0.82
PTF	0.80	0.68
TB	.95	.81
UCD	.93	.91

Table 3. Correlation Matrix and Square Roots of AVEs

PE	0.9047	0	0	0	0	0	0	0
FAM	0.4667	0.8963	0	0	0	0	0	0
IUSE	0.6723	0.3973	0.8912	0	0	0	0	0
PQ	0.7533	0.4323	0.6041	0.8040	0	0	0	0
PTF	0.7167	0.3748	0.6321	0.6821	0.5153	0.7805	0	0
TB	0.7659	0.3772	0.6746	0.7650	0.5816	0.6662	0.7856	0
UCD	0.6750	0.4933	0.5175	0.6414	0.4488	0.5805	0.6319	0.8321

.

STRUCTURAL MODELS AND HYPOTHESIS TESTING

The structural model was tested by estimating structural path coefficients and corresponding t-statistics. Bootstrapping with a two hundred re-sampling with replacement technique was used to estimate standard errors, sample mean, and path significance (Efron and Gong, 1983). It has been suggested that path coefficients of 0.20 or greater provide adequate explanatory power (Chin, 1998). Additionally, unlike covariance-based SEM, PLS models are not evaluated using model fit indices. Instead, goodness of fit for PLS models is assessed using the strength of path coefficients and R2 variance explained (Chin, 1995; Chin, 1998).

Results of Hypothesis Testing

The following figures present the path coefficients, significance of paths, and R-squares for each of the endogenous constructs used in the study. A discussion of the results of each hypothesis test is provided.

Hypothesis 1a & 1b:

In the current study context, Expectation Confirmation Theory (ECT) contends that satisfaction depends upon the extent to which users perceive their initial expectations of an IoT device to be confirmed or disconfirmed during actual use (Oliver, 1980). Therefore, we hypothesized that the confirmation/disconfirmation of a user's expectations of an IoT device's quality and effectiveness would positively impact the user's perceptions of the IoT device's quality and effectiveness. As hypothesized, ECT is a strong predictor of perceptions of quality and effectiveness; thus, Hypotheses 1a and 1b were strongly supported ($p < .01$) in the study's theoretical model.

.

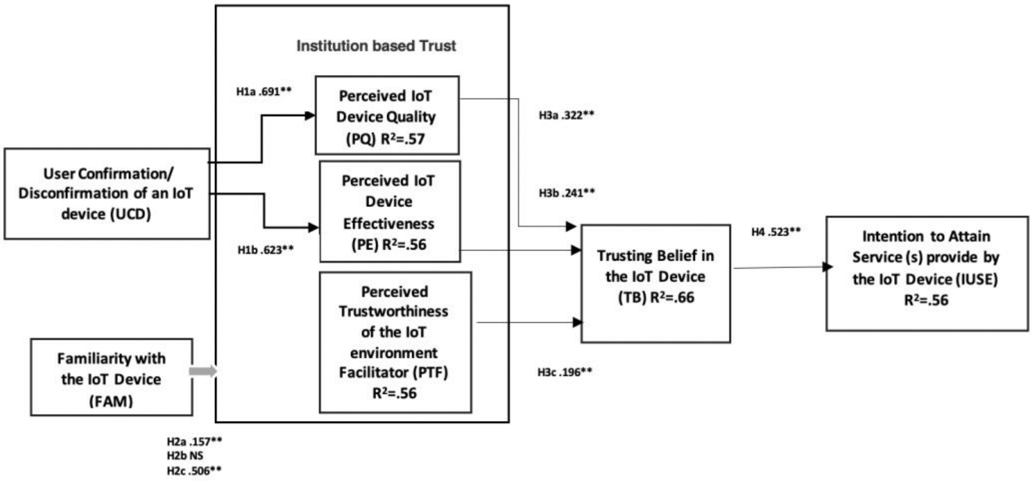
Institution based Trust
H1a .691**
Perceived IoT Device Quality (PQ) R²=.57
H3a .322**
User Confirmation/ Disconfirmation of an IoT device (UCD)
Perceived IoT Device Effectiveness (PE) R²=.56
H3b .241**
H1b .623**
H4 .523**
Trusting Belief in the IoT Device (TB) R²=.66
Intention to Attain Service (s) provide by the IoT Device (IUSE) R²=.56
Perceived Trustworthiness of the IoT environment Facilitator (PTF) R²=.56
Familiarity with the IoT Device (FAM)
H3c .196**
H2a .157**
H2b NS
H2c .506**

Figure 2. Results for the Proposed Theoretical Model

Hypothesis 2a, 2b, 2c, and 2d:

We conjecture that a user's familiarity with an IoT device will significantly affect the three constructs making up institution-based trust: perceived IoT device quality, perceived IoT device effectiveness, and perceived trustworthiness of the IoT host. Familiarity with an IoT device in the context of the current study pertains to the respondent's level of knowledge and experience with an IoT device. Results in testing Hypothesis 1a indicate that familiarity with an IoT device does have a strong and positive association with perceived IoT device quality. Familiarity derives from the user's knowledge and experience with the IoT device. In contrast, the perceived quality of an IoT device deals mainly with the user's ability to operate and navigate the system. Thus, we deduce that familiarity significantly impacted system quality perceptions from these findings.

Hypothesis 2b was not supported. Results indicate that familiarity plays a not-so-significant role in the user's perception of the effectiveness of IoT devices. Familiarity with an IoT device had a positive but not significant association with the IoT device's effectiveness, which can be described as the accuracy and reliability of the system. In the case of IoT devices, the lack of support for Hypothesis 2b stems from the way the information is collected and presented in the system. IoT devices provide essentially "second-hand" information that it has obtained from other sources to their users and present in a highly summarized fashion. Thus, users did not judge familiarity with the system as an aid in determining the accuracy and reliability of the IoT device.

.

Test data strongly supported (p<.01) Hypothesis 2c in the theoretical model evaluated across the different IoT devices. Respondents viewed familiarity as a strong predictor of the trustworthiness of the IoT environment facilitator. This finding is logical as the more familiar the user becomes with an IoT environment facilitator, the greater their opportunity to judge its trustworthiness. This result also supports existing studies that suggest that familiarity is a necessary pre-condition for trust in the online environment (Gefen, 2000).

Hypotheses 3a, 3b and 3c

Data supported all three hypotheses and posited a positive association between each of the three constructs constituting institution-based trust and trusting beliefs in IoT devices. These findings provide strong support for the influence of institution-based trust on trusting beliefs. Regarding H3a, we found that regardless of the type of IoT device used, the user's perception of the operation and navigability of the IoT devices will play an essential role in shaping trusting beliefs. Similarly, users' perception of the IoT devices' ability to provide reliable, sound, and dependable service will significantly influence trusting beliefs. Additionally, results relevant to H3c suggest that the user's perception of the IoT Facilitator's trustworthiness will significantly influence trusting beliefs in the IoT device.

Hypothesis 4

H4 is strongly supported in our model (p < .01). These findings support the positions of McKnight et al. (2002) and McKnight and Chervany (2002), who suggest that trusting beliefs will lead to trusting intentions. Hypothesis 4 suggests a positive association between trusting beliefs in an IoT device and intention to use the service provided by an IoT device.

.

FINDINGS AND DISCUSSION

We summarize our findings in the following table:

Table 4. Hypotheses Testing Results

Hypothesis	Results
H1a(UCD->PQ)	Supported
H1b(UCD-PE)	Supported
H2a(FAM->PQ)	Supported
H2b(FAM->PE)	Not Supported
H2c(FAM->PTF)	Supported
H3a(PQ->TB)	Supported
H3b(PE->TB)	Supported
H3c(PTF->TB)	Supported
H4(TB->IUSE)	Supported

All the hypotheses were strongly supported except the one between Familiarity and perceived effectiveness of IoT device. According to the study, the result for that hypothesis (H2b) was somewhat different from what was expected. The research indicates that familiarity does not play a significant role in shaping the user's perception of the effectiveness of IoT devices. Although familiarity with an IoT device has a positive association with its effectiveness, the correlation is not significant enough to be considered helpful for the user's perception of the device's accuracy and reliability.

The effectiveness of an IoT device is measured in terms of its accuracy and reliability. In the case of IoT devices, we believe the lack of support for Hypothesis 2b stems from how the information is collected and presented in the system. IoT devices provide second-hand information that they gather from other sources, and they present it in a highly summarized fashion. Therefore, users did not judge familiarity with the system as an aid in determining the accuracy and reliability of the IoT device.

The research suggests that the reason for the lack of significance in the association between familiarity and effectiveness of IoT devices is due to the nature of information presented by these devices. IoT devices collect and present the information in a highly summarized format, which means that users do not rely on their familiarity with the system to judge its accuracy and reliability. Instead, they

.

consider other factors such as the quality of information provided and the device's overall performance to determine its effectiveness.

Other than this one exception, our study found that meeting user expectations and familiarity with IoT devices are key factors in developing Institution-based Trust in an IoT environment. We tested several hypotheses and found that all but one were strongly supported. This indicates that individuals are more likely to trust IoT technology when their expectations are met, and they have prior experience with similar devices.

Furthermore, our research suggests that Institution based Trust plays a crucial role in an individual's adoption of IoT technology. When users feel that an IoT device is reliable, secure, and performs as expected, they are more likely to adopt the technology. This highlights the importance of establishing trust in IoT devices, as it can have a significant impact on their adoption and use.

Overall, our study provides valuable insights into the factors that influence trust and adoption of IoT technology. By understanding these factors, businesses and developers can design and market IoT devices that meet user expectations and build trust, ultimately leading to greater adoption and use of these technologies.

CONCLUSION

The Internet of Things (IoT) brings a new paradigm of `talking' sensors or objects with the help of the Internet. During this "talk," essential data sharing happens, which makes a user uncomfortable. Even though most consumers think the IoT can benefit them, most users are concerned about security and privacy issues and any potential data breach. Hence, the opportunities interconnected IoT devices provide are almost always accompanied by many security and privacy issues. Institution-based trust is a significant factor influencing behavioral intention to use IoT technology. Research has demonstrated that trust in institutions is crucial for users when making decisions in uncertain environments. Our proposed model has been empirically evaluated to comprehend the antecedents of institution-based trust and its role in the adoption of IoT devices in the IoT environment. Our research has shown that institution-based trust, which includes the perceived quality and effectiveness of IoT devices and the Trustworthiness of the Facilitator of the IoT environment, positively impacts the adoption of IoT. We also empirically assessed the influence of factors that affect a user's institution-based trust. Our findings indicate that when an IoT device meets a user's expectations, it increases their trust

.

in the device and encourages them to adopt it. Additionally, we observed that familiarity with the device enhances the user's perception of the device's quality and effectiveness. When we combine these two findings, the outcome tells practitioners that the Trustworthiness of IoT devices is increased if the device's design mimics devices that most users are already familiar with.

Our research has contributed significantly to the understanding of how trust in institutions plays a crucial role in increasing trust in IoT devices, ultimately affecting IoT adoption at the individual level. We have explored how institutional trust, which is defined as the trust users have in the organizations that are responsible for producing and marketing IoT devices, can influence users' trust in IoT devices and their willingness to adopt them.

Additionally, our study has addressed a critical gap in the current literature by highlighting the impact of user expectations and familiarity with a device on institutional trust in the context of IoT. We found that users' expectations of an IoT device and their familiarity with it can significantly influence their trust in the institutions that produce these devices.

Moving forward, we plan to extend our research by investigating the impact of institutional trust on various IoT devices. We also aim to enhance our proposed model by incorporating personal characteristics, such as trust levels and technological proficiency, to achieve a more comprehensive perspective. By doing so, we hope to contribute further to the understanding of how trust in institutions can facilitate IoT adoption at the individual level, and how it can be improved to promote greater confidence in IoT devices.

REFERENCES

Aaqib, M., Ali, A., Chen, L., & Nibouche, O. (2023). IoT trust and reputation: a survey and taxonomy. Journal of Cloud Computing, 12(1), 1-20.

Agarwal, R., & Venkatesh, V. (2002). Assessing a Firm's Web Presence: A Heuristic Evaluation Procedure for the Measurement of Usability. Inf. Syst. Res., 13, 168-186.

Ajzen I, Fishbein M. (1973). Attitudinal and normative variables as predictors of specific behaviors. Journal of Personality and Social Psychology. 27:41–57.

.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies*, *6*(3), 64.

Aldossari, M.Q., Sidorova, A. (2018). Consumer acceptance of Internet of Things (IoT): smart home context. Journal of Computer Information Systems 60 (6), 507-517.

Al-Momani, A.; Mahmoud, M.; Ahmad, S. Modeling the adoption of internet of things services: A conceptual framework. International. Journal of Applied Research. 2016, 2, 361–367.

Alraja, M.N., Farooque, M., & Khashab, B. (2019). 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, 7, 111341-111354.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Bagozzi, R. P., & Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. Journal of the academy of marketing science, 40, 8-34.

Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a Source of Competitive Advantage. Strategic Management Journal (15), pp. 175-190

Beldad, A.; de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, 26(5): 857-869

Cox, D., & Cox, A.D. (2002). Beyond first impressions: The effects of repeated exposure on consumer liking of visually complex and simple product designs. Journal of the Academy of Marketing Science, 30(2), 119–130.

Delgado-Ballester, E., & Hernández-Espallardo, M. (2008). Effect of Brand Associations on Consumer Reactions to Unknown On-Line Brands. International Journal of Electronic Commerce, 12(3), 81-113.

.

Esmaeilpour Ghouchani, B., Jodaki, S., Joudaki, M., Balali, A., & Rajabion, L. (2020). A model for examining the role of the Internet of Things in the development of e-business. VINE: The Journal of Information & Knowledge Management Systems, 50(1), 20.

Falcone, R.; Sapienza, A. On the Users' Acceptance of IoT Systems: A Theoretical Approach. Information 2018, 9(3) 53.

Fan, L., & Suh, Y. H. (2014). Why do users switch to a disruptive technology? An empirical study based on expectation-disconfirmation theory. *Information & Management*, *51*(2), 240-248.

Gefen, D.; Karahanna, E.; Straub, D. Trust and TAM in online shopping: An integrated model. MIS Q. 2003, 27, 51–90.

Ghoreishi, S., & Mohammadi, S. (2015). Analysis of factors that influence online trust: A unified model. World Computer Science and Information Technology Journal, 5(9), 149–154.

Giovannini, C., Ferreira, Jorge B., Silva, J., & Ferreira, D. (2015). The effects of trust transference, mobile attributes and enjoyment on mobile trust. BAR - Brazilian Administration Review, 12(1), 88-108.

Ha, Q. A., Chen, J. V., & Nguyen, T. H. T. (2021). Continuance use of enterprise social network sites as knowledge sharing platform: perspectives of tasks-technology fit and expectation disconfirmation theory. International Journal of Knowledge Management Studies, 12(4), 429-451.

Hahn, K. H., & Kim, J. (2009). The effect of offline brand trust and perceived internet confidence on online shopping intention in the integrated multi-channel context. International Journal of Retail and Distribution Management, 37(2): 126-141.

Hansen, T. (2005). Consumer adoption of online grocery buying: a discriminant analysis. International Journal of Retail & Distribution Management, Vol. 33 No. 2, pp. 101-121.

Hair, J. (2017). An updated and expanded assessment of PLS-SEM in information systems research. Industrial Management & Data Systems 117(3), 442–458.

.

Hartwick, J., and Barki, H. (1994). Explaining the Role of User Participation in Information System Use. Management Science. 40(4), pp. 440-465.

Jaspers, E. D., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. Journal of Business Research, 142, 255-265.

Karahanna, E., Straub, D. W., and Chervany, N. L. (1999). Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. MIS Quarterly 23(2), 1999, pp. 183-213.

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet Things, 15, 100420.

Keen, P., Ballance, C., Chan, S. and Schrimp, S. (2000). Electronic Commerce Relationships– Trust by Design, Prentice-Hall, Englewood Cliffs, NJ.

Khan, F., Rasli, A., Yusoff, R., & Isa, K. (2015). Impact of trust on online shopping: A systematic review of literature. Journal of Advanced Review on Scientific Research, 8(1), 1–8.

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.

Kim, D., & Benbasat, I. (2006). The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation. Information Systems Research, 17(3), 286-300

Kim, G., Shin, B., & Lee, H. G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. Information Systems Journal, 19(3), 283-311.

Koohang, A., Sargent, C.S., Nord, J.H., Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use International Journal of Information Management, 62.

.

Kuan, H-H., & Bock, G-W. (2007). Trust transference in brick and click retailers: an investigation of the before-online-visit phase. Information and Management, 44(2): 175-187.

Kumar, V. Ramachandran, D., Kumar, B. (2020). Influence of new-age technologies on marketing: A research agenda Journal of Business Research., 125 pp. 864-877, 10.1016/j.jbusres.2020.01.007

Lee, M. (2019). An Empirical Study of Home IoT Services in South Korea: The Moderating Effect of the Usage Experience. International Journal of Human-Computer Interaction. 2019, Vol. 35 Issue 7

Leonard, L. N., & Jones, K. (2021). Trust in C2C Electronic Commerce: Ten Years Later. Journal of Computer Information Systems, 61(3).

Lim, K., Sia, C. L., Lee, M. K. O., and Benbasat, I. (2006). How Do I Trust You Online, and If So, Will I Buy? An Empirical Study on Designing Web Contents to Develop Online Trust. Journal of Management Information Systems (23:2), pp. 233-266.

Lin, J.; Lu, Y.; Wang, B., & Wei, K. K. (2011). The role of inter-channel trust transfer in establishing mobile commerce trust. Electronic Commerce Research and Applications, 10(6): 615-625.

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. Proceedings on Privacy Enhancing Technologies, 2019(4), 250-271.

Mari, A., & Algesheimer, R. (2021). The role of trusting beliefs in voice assistants during voice shopping.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. “An Integrative Model of Organizational Trust,” Academy of Management Review (20), 1995, pp. 709-734.

McKnight, D.H., Cummings, L.L., Chervany, N.L. (1998). Initial trust formation in new organizational relationships. Academy of Management Review 23 (3), 473–490.

McKnight, D. H; Choudhury, V; and Kacmar, C. (2000). Trust in E-Commerce Vendors: A Two-Stage Model. ICIS 2000 Proceedings. 54.

.

McKnight, D. H. & Chervany, N. (2000). What is Trust? A Conceptual Analysis and an Interdisciplinary Model. AMCIS 2000 Proceedings. Paper 382.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology. ACM Transactions on Management Information Systems 2(2), 1–25.

Menard, P., & Bott, G. (2018). Investigating Privacy Concerns of Internet of Things (IoT) Users. Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018.

Menon, N.M., Konana, P., Browne, G.J., Balasubramanian, S. (1999). Understanding trustworthiness beliefs in electronic brokerage usage. In: De, P., DeGross, J.I. (Eds.), Proceedings of the 20th International Conference on Information Systems, December 13–15, pp. 552–555.

Meyerson, D., Weick, K.E., Kramer, R.M. (1996). Swift trust and temporary groups. In: Kramer, R.M., Tyler, T.R. (Eds.), Trust in Organizations: Frontiers of Theory and Research, Sage, Thousand Oaks, CA, pp. 166–195.

Mishra, A.K. Organizational responses to crisis: The centrality of trust. In R.M. Kramer and T.R. Tyler (eds.), Trust in Organizations: Frontiers of Theory and Research. Thousand Oaks, CA: Sage, 1996, pp. 261–287.

Nord, J.H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. Expert Syst. Appl., 133, 97-108.

Pal, D., Funilkul, S., & Papasratorn, B. (2019). Antecedents of Trust and the Continuance Intention in IoT-Based Smart Products: The Case of Consumer Wearables. IEEE Access, 7, 184160-184171.

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. Information Systems Research, 15(1), 37–59.

Pavlou, P. A. (2002). Institutional trust in interorganizational exchange relationships: The role of electronic B2B marketplaces. J. Strategic Inform. Systems 11(3–4) 215–243.

.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. Internat. Journal. Electronic Commerce 7(3) 69–103.

Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. (2014). Context Aware Computing for The Internet of Things: A Survey. IEEE Commun. Surv. 16, 414–454.

Rheu, M., Shin, J. Y., Peng, W., & Huh-Yoo, J. (2021). Systematic review: Trust-building factors and implications for conversational agent design. International Journal of Human–Computer Interaction, 37(1), 81-96.

Riemenschneider, D., Harrison, D. and Mykytyn, P. (2003). Understanding IT adoption decisions in small business: integrating current theories. Information Management, Vol.40, pp.269–285.

Ratnasingam, P., & Pavlou, P. (2002). Technology trust: The next value creator in B2B electronic commerce. International Resource Management Association Conference: Seattle, Washington, May 21- 23.

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. Journal of the Academy of Marketing Science, 30(4), 455-464.

Salam, A.F., Iyer, L., Palvia, P. and Singh, R. (2005). Trust in e-commerce, Communications of the ACM, 48(2), 73-77.

Shao, Z., & Yin, H. (2019). Building customers' trust in the ridesharing platform with institutional mechanisms: An empirical study in China. Internet Research, 29(5), 1040-1063.

Sim, J. J., Chia, Z. Y., Chin, Y. L., Lee, M. Q., Chiam, V. T. S., Wong, K. L., & Yeap, K. H. (2018, November). Trust in vendor and perceived effectiveness of E-commerce institutional mechanisms in M-commerce adoption: A revised UTAUT model. In 2018 8th IEEE international conference on control system, computing and engineering (ICCSCE) (pp. 10-15). IEEE.

Song J., & Zahedi F. (2005). A theoretical approach to web design in e-commerce: a belief reinforcement model, Management Science, 51(8) 1219-1235.

.

Stewart, K. J. (2003). Trust transfer on the World Wide Web. *Organization Science, 14*(1), 5–17.

Stewart, K. J. (2006). How Hypertext Links Influence Consumer Perceptions to Build and Degrade Trust Online, Journal of Management Information Systems, 23(1).

Tandon, U., Mittal, A., & Manohar, S. (2021). Examining the impact of intangible product features and e-commerce institutional mechanics on consumer trust and repurchase intention. Electronic Markets, 31, 945-964.

Thapa, S., Bello, A., Maurushat, A., & Farid, F. (2023). Security Risks and User Perception towards Adopting Wearable Internet of Medical Things. International Journal of Environmental Research and Public Health, 20(8), 5519.

Venkatesh, V., Morris, M., Davis, G.B., and Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27(3) pp. 425-78.

Venkatesh, V., & Morris, M. (2000). Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior. MIS Quarterly, 24(1), 115-139.

Voas, J., Kuhn, R., Laplante, P., & Applebaum, S. (2018). Internet of Things (IoT) Trust Concerns. Gaithersburg, Maryland. Retrieved from https://csrc.nist.gov/publications

Wang, X., Zhou, R., & Zhang, R. (2020). The impact of expectation and disconfirmation on user experience and behavior intention. In Design, User Experience, and Usability. Interaction Design: 9th International Conference, DUXU 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part I 22 (pp. 464-475). Springer International Publishing.

Wang, X. (2022). Comparing Traditional Commerce to E-Commerce and IoT and the Understanding of Trust for the Consumer, Wireless Communications and Mobile Computing, vol. 2022, Article ID 1811984, 7 pages, 2022. https://doi.org/10.1155/2022/1811984.

.

Yildirima, H.; Ali-Eldina, A. A model for predicting user intention to use wearable IoT devices at The workplace. J. King Saud Univ. Computer. Inf. Sci. 2018.

Yuliati, L. N., Dradjat, H. A., & Simanjuntak, M. (2020). Online bike: Role of perceived technology, perceived risk, and institution-based trust on service usage via online trust. Cogent Business & Management, 7(1), 1798067.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), [200].

Zubiaga A, Procter R, Maple C. (2018). A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things. PLoS ONE 13(12): e0209472. https://doi.org/10.1371/journal.pone.0209472.

Zucker, L.G. (1986). The Production of Trust: Institutional Sources of Economic Structure, 1840-1920. Research in Organizational Behavior, 8, 53-111.

.