Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Research Article

Internet of Things (IoT): From awareness to continued use

Alex Koohang [a,*], Carol Springer Sargent [a], Jeretta Horn Nord [b], Joanna Paliszkiewicz [c]

[a] *Middle Georgia State University, USA*
[b] *Oklahoma State University, USA*
[c] *Warsaw University of Life Sciences, Poland*

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Privacy
Security
Trust
Intention to use IoT
Awareness

ABSTRACT

This paper proposes a research model with five constructs, i.e., IoT awareness, users' IoT privacy knowledge, users' IoT security knowledge, users' IoT Trust, and continued intention to use IoT to bring clarity to the growing yet fragmented literature on the path from IoT awareness to the continued use of IoT. Hypotheses stemming from the proposed model were stated. A total of 297 subjects from various organizations in 9 regions of the USA participated in the study. Collected data were analyzed through path modeling, using SmartPLS 3.0. The results indicated that IoT awareness can positively influence users' knowledge of IoT privacy and security. The users' knowledge of IoT privacy and security can positively influence users' IoT trust and subsequently, the users' IoT trust can positively influence continued intention to use IoT. Additionally, IoT privacy knowledge, IoT security knowledge, and IoT trust were found to be the mediating variables in the proposed model. Theoretical and practical implications of findings, as well as recommendations for further research, are discussed.

1. Introduction

Internet of Things (IoT) describes a vast array of objects with sensing and actuating devices that collect, analyze and share data across other objects, programs, and platforms. IoT, the biggest emerging trend in technology, has launched an unprecedented information revolution (Nord, Koohang, & Paliszkiewicz, 2019). It is one of the most notable disruptive technologies of this century and has caught the attention of the academy, society, and the industry (Brous, Janssen, & Herder, 2020; Kassab, DeFranco, & Laplante, 2020; Nord et al., 2019). Mattern and Floerkemeier (2010) define the IoT as the items connected to the virtual world where they are "controlled remotely and can act as physical access points to the Internet services." Huang, Craig, Lin, and Yan (2016) defined it as "a worldwide network of physical objects using the Internet as a communication media." Ben-Daya, Hassini, and Bahroun (2019) described it as "… a network of physical objects that are digitally connected to sense, monitor, and interact within a company and between the company and its supply chain enabling agility, visibility, tracking, and information sharing to facilitate timely planning, control, and coordination of the supply chain processes.".

From 2012–2018, the use of IoT devices grew from 8.7 billion to 50.1 billion even though adoptions in homes and retail areas were still relatively sparse (Bansal, Chana, & Clarke, 2020; Burhan, Rehman, Khan, & Byung-Seo, 2018), spawning spending likely north of a trillion dollars annually (Bansal et al., 2020; Baranwal, Singh, & Vidyarthi, 2020). Smartphones, as a part of IoT smart devices, have played a significant role in this growth. These smart devices offer more than personal benefits, they can boost autonomy, improve communication, and facilitate knowledge sharing that lead to enhanced job satisfaction and productivity in the workplace (Pitichat, 2013). The IoT devices owned by employees are increasingly used in the workplace for performing day-to-day business activities and productivity apps are the most dominant kind of apps on users' smartphones used in the workplace. Moreover, many IT executives believe that smartphones are highly important to increased employee productivity as they improve business processes (Lellis, 2020). The increased usage of IoT devices in the workplace brings with it deep concern over attacks, threats, and exploits (Asad, Moustafa, & Yu, 2020; Bansal et al., 2020; Duan & Guo, 2021; Ren, Li, Dai, Yang, & Lin, 2018; Vignau, Khoury, Hallé, & Hamou-Lhadj, 2021; Waheed, Xiangjian, Ikram, Usman, & Hashmi, 2020; Zhang, Zhong, Shi, & Liu, 2021).

Among the many challenges this massive increase in IoT device use brings, Nord et al. (2019) identified three pervasive challenges - privacy, security, and trust. These IoT challenges can impact the IoT users'

[*] Corresponding author.
E-mail addresses: alex.koohang@mga.edu (A. Koohang), carol.sargent@mga.edu (C.S. Sargent), jeretta.nord@okstate.edu (J.H. Nord), joanna_paliszkiewicz@sggw.edu.pl (J. Paliszkiewicz).

https://doi.org/10.1016/j.ijinfomgt.2021.102442
Received 16 September 2021; Received in revised form 10 October 2021; Accepted 14 October 2021
Available online 28 October 2021

intended use (Hsu & C.-L, 2016a; Nord et al., 2019). Security, privacy, and trust in the IoT have been studied widely (Alaiad & Zhou, 2017; Bansal et al., 2020; Celik, Fernandes, Pauley, Gang, & McDaniel, 2019; Duan & Guo, 2021; Hsu & Lin, 2018; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Vignau et al., 2021). Guo, Chen, and Tsai (2017) stated that privacy, security, and trust are crucial to the success of IoT, however, privacy and security are precursors to trust. Furthermore, Nord et al. (2019) indicated that IoT user trust can increase only if IoT privacy and security knowledge are addressed. The literature has widely mentioned the importance of users' IoT awareness on users' IoT privacy and security (Adjerid, Peer, & Acquisti, 2018; Alasdair, 2017; Chen & Wen, 2019; Rice & Bogdanov, 2019). While IT professionals have knowledge that makes them aware of the security and privacy issues surrounding IoT, end users may not have the awareness or the skills to process the level of privacy and security threats inherent in their device use or in their IoT service providers that host the data harvested off these devices (Adjerid et al., 2018; Alasdair, 2017; Chen & Wen, 2019; Rice & Bogdanov, 2019).

What is missing from the growing yet fragmented literature is the clarity of how these challenges, i.e., privacy, security, and trust specifically link from IoT awareness to IoT continued use. Therefore, our goal is to examine how IoT awareness affects IoT privacy, IoT security, and IoT trust which in turn affect continued intention to use IoT. Consistent with its goal, this paper is organized as follows. We begin with a review of the literature that proceeds with a proposed research model and hypothesis development. Next, the methodology is presented following the results. Subsequently, the findings are discussed following their theoretical and practical implications. Finally, limitations, future research directions, and conclusions round out the paper.

2. Literature review

Technology professionals agree that IoT devices present major security and privacy issues and the literature on possible solutions grows annually (Babun, Denney, Celik, McDaniel, & Uluagac, 2021; Celik et al., 2019; Duan & Guo, 2021; Ghosh, Edwards, & Hosseini, 2021). Device security has been a low priority for manufacturers, leaving end-users and decision-makers with the burden of deciding whether to take data risk as a trade-off for receiving the functionality of the device (Hsu & Lin, 2018; Johnson, Blythe, Manning, & Wong, 2020; Lee, 2020). IoT security issues involve devices' ability to disrupt other technology, attack users' devices and systems, and validate access control (Celik et al., 2019; Duan & Guo, 2021; Vignau et al., 2021). Many IoT devices, like vehicles, are left unattended in public places, making them even more vulnerable to physical attacks (Jiang et al., 2021). Edge devices run up against issues of anonymity, traceability, and integrity of the data collected (Fang & Feng, 2021). End users, decision-makers, and platform managers want assurance that the sharing of device settings, activity, and ownership occurs only with the user's knowledge and permission (Fang & Feng, 2021).

Models predicting intention to use IoT include a laundry list of challenges with privacy and security figuring prominently in all (Alaiad & Zhou, 2017; Kelly, Campbell, Gong, & Scuffham, 2020). In a staggering array of possible uses, security and privacy surface as key features for intention to use such as in healthcare (Attarian & Hashemi, 2021; Bica, Chifor, Arseni, & Matei, 2019), construction (Ghosh et al., 2021; Oke, Arowoiya, & Akomolafe, 2020) homeowner applications (Touqeer et al., 2021), smartwatches (Mani & Chouk, 2017), commercial buying (Osmonbekov & Johnston, 2018), manufacturing (Ranjan, Jha, & Pal, 2017), waste management, and smart cities (Sharma et al., 2020; Weber & Podnar Žarko, 2019; Wirtz, Weyerer, & Schichtel, 2019). In a research study involving 495 IoT users, the perceived privacy issues lowered perceived IoT value and IoT intention to use (Hsu & Lin, 2018).

2.1. Device threat vs. service provider threat

The literature blends the security and privacy risks of the device (perception layer) with the service provider layer (network layer). Users, in general, indicate security and privacy are critical issues, regardless of the layer that opens those risks. For IT professionals, the source of threats matters a great deal as improving security and privacy requires identifying the location of the vulnerabilities (Bica et al., 2019; Burhan et al., 2018; Waheed et al., 2020; Weber & Podnar Žarko, 2019).

Research has provided some insight into how decision-makers view service providers (vs. device providers). The list of potential quality indicators in selecting IoT service providers includes privacy and security as well as the performance of the system, disaster recovery, availability, interoperability, pricing, and customer support (Baranwal et al., 2020). For some decision-makers, the internet or cloud service provider, not the device e-provider, is the gatekeeper that needs to control the privacy and security of the end-user data (Bansal et al., 2020; Lee, 2020). These intermediaries, having access to all user data, not just specific device-generated data, have vast unregulated power to mine user data, perhaps leading to end-users avoiding all IoT from lack of trust in their ability to control their personal data (Lundqvist, 2019).

IT professionals and some savvy non-IT users and decision-makers recognize these distinct risk layers, including collection, storage, analysis, and utilization of information from IoT devices (Ando, Shima, & Takemure, 2016). We know little about whether end users have knowledge about service-provider threats, device-specific threats, or threats from any layer or source. Many important IoT solutions are still at the Proof-of-Concept (PoC) stage. While consumers perceive high value in IoT, they simultaneously report low trust in IoT data exchange (Bansal et al., 2020). Getting widespread use will require addressing the pervasive privacy and security risks of decision-makers and end-users, starting with granularity in which source of risk weighs heavily on users. IT professionals need a better understanding of how these bear on decision-making for IoT devices.

3. Hypothesis development

The purpose of this paper is to propose a research model with five constructs, i.e., IoT awareness, users' IoT privacy knowledge, users' IoT security knowledge, users' IoT Trust, and continued intention to use IoT (See Fig. 1). Via path modeling, we assert that IoT awareness can positively influence users' awareness of IoT privacy knowledge and users' IoT security knowledge. The users' awareness of IoT privacy knowledge and IoT security knowledge can positively influence users' IoT trust. Finally, users' IoT trust can influence continued intention to use IoT. Table 1 shows the descriptions and sources of the constructs.

3.1. IoT awareness

User awareness of IoT threats is evolving. Since 2008, Data Privacy Day (January 28th) has promoted consumer and community awareness of privacy and security controls over data (ISACA, 2019; Marketwired, 2015). This awareness continues to grow with a steady drumbeat of headlines about malicious attacks ranging from extremes of "hacking the planet" to malicious accessing of household items such as baby monitors or lightbulbs (Almusaylim & Zaman, 2019; Dubno, 2017; Economist, 2019; Kerner, 2017; Polat & Du, 2005; Schneier, 2017; Urrico, 2018).

User awareness, however, shows mixed results. In a 2016 study, nearly half of consumers cited privacy as a barrier to IoT use, showing strong awareness (Newswire, 2016b). By contrast, a study conducted by Rice and Bogdanov (2019) showed that users were generally ill-informed about ways their data might be misused. Some users just want the devices to work easily with little effort, taking little interest in the technology threats behind the devices (Alasdair, 2017). Historically, IoT devices were not fully "do it yourself", creating mostly users with some technology awareness (Alasdair, 2017). That is, however,

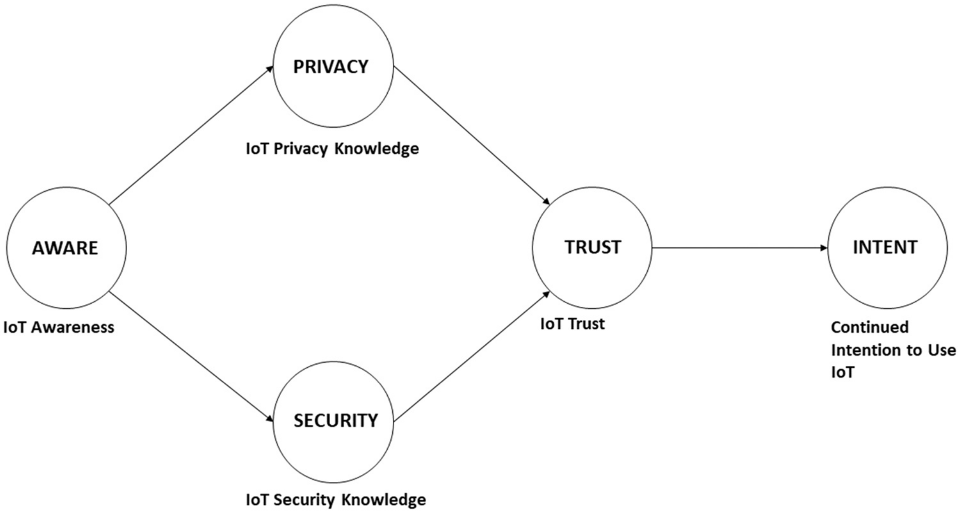

Fig. 1. Proposed research model.

Table 1
Definitions of constructs.

Construct	Definition	Source (s)
IoT Awareness	IoT awareness is defined as the degree to which users are aware of and have the basic knowledge of growing security/privacy threats of IoT that they may encounter on a regular and routine basis.	Designed for the present study.
IoT Privacy Knowledge	IoT privacy knowledge is defined as the degree to which users of IoT devices have knowledge about the unauthorized collection, secondary storage, and improper access of their personal information by IoT service providers.	Adapted and modified for IoT privacy knowledge from Koohang, Paliszkiewicz, and Goluchowski (2018)
IoT Security Knowledge	IoT security knowledge is defined as the degree to which users of IoT devices have the knowledge of whether IoT service providers safeguard them against IoT security vulnerabilities to keep attackers from infiltrating their IoT devices and networks.	Adapted from Zhang and Gupta (2018) and modified for IoT security knowledge
IoT Trust	IoT trust is defined as the degree to which users of IoT devices trust that the IoT service providers that provide products and applications are trustworthy, benevolent, and skillful enough in protecting the users against security/privacy threats and risks.	Adapted from Koohang, Nowak, Paliszkiewicz, and Nord (2020) and modified for IoT trust
Continued Intention to Use IoT	Continued intention to use IoT services is defined as the degree to which users of IoT devices believe that they will continue using IoT services.	Adapted & Modified from Hsu and C.-L (2016a)

changing with more plug-and-play devices, creating two classes of users, more aware and less aware. Many users innocently surrender to device prompts without reading terms and conditions when downloading applications (Alasdair, 2017).

3.2. IoT privacy and security knowledge

Privacy is the right to decide who gets to know personal information about the user (Hsu & C.-L, 2016a). Privacy spans many areas, including identity privacy, data privacy, attribute privacy, and task privacy (Wang, Yan, Feng, & Liu, 2020). Non-static data that is subject to update, deletion, or insertion creates privacy preservation issues (Song, Ju, Zhu, & Li, 2021; Tinamas & Natwichai, 2020). Privacy includes not just user-initiated tasks and data, but also crowd-sensing technology, which accesses devices to harvest location data without user consent (Li & Shin, 2018) and using personal data for unexpected purposes (Ando et al., 2016). Privacy and security awareness have increased the pressure to address security and privacy so that users do not opt-out of device use (Karwatzki et al., 2017; Newswire, 2015; Rashid et al., 2020).

The literature documents the importance of users' IoT awareness, i.e., awareness of the skills to process the level of privacy and security threats inherent in their IoT devices and service providers (Adjerid et al., 2018; Alasdair, 2017; Chen & Wen, 2019; Rice & Bogdanov, 2019). The literature also widely documents the significance of users' IoT privacy and security (Alaiad & Zhou, 2017; Bansal et al., 2020; Celik et al., 2019; Duan & Guo, 2021; Hsu & Lin, 2018; Vignau et al., 2021).

In the present study, IoT awareness is defined as the degree to which users know the basics of growing security/privacy threats of IoT that they may encounter on a routine basis. Moreover, IoT privacy knowledge is defined as the degree to which users of IoT devices know about the unauthorized collection, secondary storage, and improper access of their personal information by IoT service providers.

Additionally, IoT security knowledge is defined as the degree to which users of IoT devices know whether IoT service providers safeguard them against IoT security vulnerabilities to keep attackers from infiltrating their IoT devices and networks. Given the above, we assert that the IoT awareness can positively influence users' IoT privacy knowledge and state the following hypotheses:

H1. Users' IoT awareness affect their IoT privacy knowledge.

H2. Users' IoT awareness affect their IoT security knowledge.

3.3. IoT trust

Using IoT devices require some loss of control as the device makes decisions for the consumer, prompting trust issues (Alasdair, 2017). To build trust, users want to be notified when their data is accessed and want to know the policies that dictate the management of their data as it moved and is stored between devices and networks (Ando et al., 2016;

Polat & Du, 2005; Rashid, Conzon, Tao, & Ferrera, 2020; Wang, 2019).

Trust in a network stems from users' perception that they are "safe." That is, that the user is spared from attacks to their system (security) and unauthorized access to their data (privacy) (Tikhvinskiy & Bochechka, 2017; Yarali, Yedla, Almalki, Covey, & Almohanna, 2017). As many as half of consumers hesitate to use IoT devices due to a lack of trust stemming from privacy and security issues (Newswire, 2016a). IoT devices with inadequate security erode consumer trust and inhibit IoT use (Alasdair, 2017).

Trust involves not just trustworthy devices but trust in the IoT network as a whole (Alshehri & Hussain, 2019). The network comprises interactions of autonomous homogeneous and heterogeneous nodes, any of which may be prone to threats, making trust highly dependent on the security and privacy performance of the interacting entities (Ferraris & Fernandez-Gago, 2020; Hamdani et al., 2021).

To ensure user trust of device threat, the quality of experience or quality of service for users requires ensuring the protection of users' privacy and security (Li et al., 2021). As the public has become more knowledgeable about how devices and networks attend to threats that can potentially expose their identity and their data to others, trust rises (Russell & Van Duran, 2018; Sanfilippo, Shvartzshnaider, Reyes, Nissenbaum, & Egelman, 2020; Yarali et al., 2017). In response to users' need for assurance that they can trust devices that cross diverse platforms and applications, organizations conduct privacy impact assessments to assess privacy risks, especially when devices cross diverse platforms and applications, to help users trust providers (Rashid et al., 2020).

In the present study, IoT trust is defined IoT as the degree to which users of IoT devices trust that the IoT service providers that provide products and applications are trustworthy, benevolent, and skillful enough in protecting the users against security/privacy threats and risks. Given the importance of IoT trust in relation to IoT privacy and security knowledge, we assert that users' IoT privacy and security knowledge influence their IoT trust and state the following hypotheses.

H3. Users' IoT privacy knowledge affect their IoT trust.

H4. Users' IoT security knowledge affect their IoT trust.

3.4. *Intention to use IoT*

Continued use of IoT services depends upon several factors, i.e., performance expectation, life quality expectation, human detachment concerns, social influence, privacy, cost emotional support, and psychological concern (Alaiad & Zhou, 2017; Chatterjee, Kar, & Dwivedi, 2021; Gao & Bai, 2014; Mani & Chouk, 2017; Tsourela & Nerantzaki, 2020). Even when benefits are strong, users report lower intention to use if they have low trust perceptions (Ando et al., 2016; Arfi, Nasr, Kondrateva, & Hikkerova, 2021; Lee, 2020). In Japan, when service providers pass a third-party inspection on privacy/security, they display a "PrivacyMark" seal of trust on their website to reduce anxiety about site use (Ando et al., 2016). Experiments have shown that intention to buy increases with the brand (e.g., device) trust and vendor (e.g., service provider) trust, as separate predictors of intention to use (Becerra & Korgaonkar, 2011). Other studies reveal that trust in online platforms increases the intention to buy (Ha, Huong, Nguyen, & GNguyen, 2019; Ling, Chai, & Piew, 2010). In a model of cloud services, high trust (security) factored significantly in decisions to use (Hsu & C.-l, 2016b).

In the present study, continued intention to use IoT services is defined as the degree to which users of IoT devices believe that they will continue using IoT services. Jayashankar, Nilakanta, Johnston, Gill, and Burres (2018) stated that user trust influences perceived value and threats in IoT environments that in turn influences IoT use. Trust in IoT environments reduces uncertainty and threats, thus generating a sense of safety (Lin, 2011). User trust in IoT technologies is believed to play a pivotal role in the continued intention to use IoT (Gao & Bai, 2014; Tsourela & Nerantzaki, 2020). Therefore, we assert that users' trust influences continued intention to use IoT services and state the following hypothesis:

H5. Users' IoT trust affect their continued intention to use IoT.

3.5. *Mediation*

Carrión, Nitzl, and Roldán (2017) stated that mediation or indirect effect examines whether there is a relationship between the independent and dependent variables in a model. A mediating effect exists when a third variable acts as a mediator between two other related latent variables/constructs (Carrión et al., 2017; Hair, Risher, Sarstedt, & Ringle, 2019). We, therefore, assert that the discovery of mediating effect between the variables in our research model can provide knowledge to understand the nature of the relationship between two constructs and state the following hypothesis:

H6. Mediation relationship in the research model exists between the independent and dependent variables.

4. Methodology

4.1. *Measures*

This study uses four constructs. They are IoT Awareness with 3 items, designed for the present study. IoT Privacy Knowledge with 3 items, adapted and modified for IoT privacy knowledge from Koohang et al. (2018). IoT Security Knowledge with 3 items, adapted from Zhang and Gupta (2018) and modified for IoT security knowledge. IoT Trust with 3 items, adapted from Koohang et al. (2020) and modified for IoT trust. Continued Intention to Use IoT with 2 items, adapted & Modified from Hsu and C.-L (2016a). The definitions of the constructs are shown in Table 1. The items of the constructs are shown in Appendix A. The following scoring strategy was used: 7 = Completely Agree, 6 = Mostly Agree, 5 = Somewhat Agree, 4 = Neither Agree nor Disagree, 3 = Somewhat Disagree, 2 = Mostly Disagree, and 1 = Completely Disagree.

4.2. *Subjects*

The survey instrument was administered electronically by a professional Internet survey organization to approximately 1000 subjects using IoT products and applications through various devices at the workplace. The subjects were from various organizations in 9 different regions in the USA. We received 299 completed surveys. Of the 299, 2 were eliminated as a result of the outlier analysis of the data. This yielded a final total of 297 subjects for the study. All subjects were guaranteed confidentiality and anonymity. See Table 2 for the complete demographics of the subjects.

4.3. *Data analysis*

SmartPLS 3.0 (Ringle, Wende, & Will, 2005), partial least square structural equation modeling (PLS-SEM) was used to analyze the data. The analyses include confirming the reliability and validity of the research model and assessing the structural model that encompasses coefficient of determination (R^2) and blindfolding-based cross-validated redundancy measure (Q^2). These analyses determine the strength of the research model. Next, the path coefficients, *t*-statistics, and *p*-values are assessed to determine the acceptance or rejection of the hypotheses. Finally, the mediating effect (indirect effect) is assessed to determine the relationship between the variables in the research model.

Table 2
Demographics (N = 297).

Average daily time spent on the IoT (products/applications) via various devices	*N*	%
1–2 h	91	30.6
3–4 h	108	36.4
5–7 h	56	18.9
Over 7 h	42	14.1
Likely daily use of the IoT (products/applications) via various devices	***N***	**%**
Extremely likely	109	36.7
Very likely	79	26.6
Moderately likely	68	22.9
Slightly likely	41	13.8
Company Activity	***N***	**%**
Manufacturing	30	10.1
Banking/Financial Services	17	5.7
Insurance	9	3.0
Tech/Computer Software	32	10.8
Healthcare/Medical	57	19.2
Retail	7	2.4
Government	20	6.7
Services	59	19.9
Other	66	22.2
Age	***N***	**%**
18–29	80	26.9
30–44	86	29.0
45–60	99	33.3
Above 60	32	10.8
Gender	***N***	**%**
Male	159	53.54
Female	135	45.45
Prefer not to say	3	1.01
Job Level	***N***	**%**
Owner / Executive / C-Level	37	12.5
Senior Management	24	8.1
Middle management	77	25.9
Intermediate	88	29.6
Entry Level	71	23.9
Number of Employees in Company	***N***	**%**
1–50	102	34.3
51–500	68	22.9
501–2000	51	17.2
2000–10,000	43	14.5
Over 10,000	33	11.1
Region	***N***	**%**
New England	60	20.2
Middle Atlantic	16	5.4
East North Central	49	16.5
West North Central	11	3.7
South Atlantic	15	5.1
East South Central	54	18.2
West South Central	57	19.2
Mountain	13	4.4
Pacific	22	7.4

5. Results

5.1. Conforming the reliability of the research model

According to Hair et al. (2019), the reliability of the research model is confirmed by the indicator reliability and internal consistency. The indicator reliability is achieved when the outer loadings of all indicators for each latent variable/construct are.70 or greater. The internal consistency is achieved when the composite reliability for each latent variable/construct is equal to or greater than.70.

Table 3 shows the results of indicator reliability and internal consistency establishing the reliability of the research model where all indicators for each latent variable/construct are above the threshold value of.70 and the composite reliability for each latent variable/construct is above the threshold value of.70.

5.2. Confirming the Validity of the research model

To confirm the validity of the research model, convergent validity and discriminant validity are assessed. According to Hair et al. (2019), convergence validity exists when the average variance extracted (AVE) for each latent variable / construct is above 0.5. The AVEs for the latent variables / constructs are AWARE = 0.846, PRIVACY = 0.835, SECURITY = 0.820, TRUST = 0.617, and INTENT = 0.904 achieving the convergent validity of the research model.

The discriminant validity is determined by assessing three procedures – the Fornell-Larcker criterion where the square root of the AVE of each latent variable/construct is higher than its highest correlation with any other latent variable/constructs; the cross-loadings where an indicator's outer loading on a latent variable is higher than all its cross-loadings with other latent variables; and the heterotrait-monotrait ratio of correlations (HTMT) where the results for all values are below the threshold value of 0.9 (Hair et al., 2019).

Tables 4, 5, and 6, show the results for Fornell-Larcker criterion, cross-loadings, and the heterotrait-monotrait ratio of correlations (HTMT). These results indicated the achievement of discriminant validity of the research model.

Table 4
Fornell-Larcker criterion.

	AWARE	PRIVACY	SECURITY	TRUST	INTENT
AWARE	0.920				
PRIVACY	0.698	0.914			
SECURITY	0.733	0.731	0.906		
TRUST	0.249	0.279	0.291	0.786	
INTENT	0.716	0.703	0.689	0.282	0.951

Table 3
Reliability.

	Indicators	Outer Loadings	Cronbach's Alpha	rho_A	Composite Reliability
IoT Awareness (AWARE)	AWARE1	**0.912**	**0.909**	**0.909**	**0.943**
	AWARE2	**0.930**			
	AWARE3	**0.917**			
IoT Privacy Knowledge (PRIVACY)	PRIVACY 1	**0.907**	**0.901**	**0.902**	**0.938**
	PRIVACY 2	**0.926**			
	PRIVACY 3	**0.907**			
IoT Security Knowledge (SECURITY)	SECURITY 1	**0.906**	**0.890**	**0.891**	**0.932**
	SECURITY 2	**0.905**			
	SECURITY 3	**0.906**			
IoT Trust (TRUST)	TRUST1	**0.767**	**0.705**	**0.715**	**0.828**
	TRUST2	**0.746**			
	TRUST3	**0.841**			
IoT Intention to Use (INTENT)	INTENT1	**0.951**	**0.893**	**0.893**	**0.949**
	INTENT2	**0.950**			

Table 5
Cross-loadings.

	AWARE	PRIVACY	SECURITY	TRUST	INTENT
AWARE1	**0.912**	0.674	0.676	0.252	0.654
AWARE2	**0.930**	0.635	0.677	0.202	0.662
AWARE3	**0.917**	0.615	0.669	0.232	0.658
PRIVACY 1	0.652	**0.907**	0.674	0.260	0.649
PRIVACY 2	0.646	**0.926**	0.697	0.257	0.664
PRIVACY 3	0.615	**0.907**	0.631	0.247	0.613
SECURITY 1	0.684	0.658	**0.906**	0.236	0.651
SECURITY 2	0.671	0.686	**0.905**	0.264	0.605
SECURITY 3	0.635	0.641	**0.906**	0.293	0.614
TRUST1	0.219	0.303	0.284	**0.767**	0.258
TRUST2	0.182	0.133	0.183	**0.746**	0.191
TRUST3	0.172	0.173	0.187	**0.841**	0.194
INTENT1	0.674	0.689	0.662	0.269	**0.951**
INTENT2	0.686	0.647	0.647	0.267	**0.950**

Table 6
Hetrotrait-Monotrait ratio of correlations (HTMT).

	AWARE	PRIVACY	SECURITY	TRUST	INTENT
AWARE					
PRIVACY	0.770				
SECURITY	0.814	0.815			
TRUST	0.300	0.321	0.348		
INTENT	0.794	0.783	0.772	0.340	

5.3. *Assessing the structural model*

(Hair et al., 2019) stated that the variance inflation factor (VIF) for all the predictor constructs should be examined before assessing the structural model. The VIF results for the predictor constructs assures that there are no collinearity issues that bias the regression results. To achieve this, the VIF value for each predictor construct should be below 3.0. The VIF for all predictor constructs was below the threshold value of 3.0 (from 1.000 to 2.147), showing the non-collinearly of the research model.

The structural model was assessed with coefficient of determination (R^2), the blindfolding-based cross-validated redundancy measure (Q^2), and the path coefficients. The R^2 values measuring the variance explained in each of the predictor constructs were PRIVACY = 59%, SECURITY = 66%, TRUST = 14%, and INTENT = 0.60% suggesting a collective moderate to high values (Hair et al., 2019). The Q^2 values for each endogenous construct, according to Hair et al. (2019), must be higher than zero to indicate the predictive accuracy of the structural model for that construct. The Q^2 values for the endogenous constructs in the research model were PRIVACY = 0.48, SECURITY = 0.53, TRUST = 0.050 and INTENT = 0.10 suggesting a well-grounded predictive relevance for the research model.

The path coefficients, *t*-Statistics, and *p*-values are shown in Table 7. Hypothesis 1 that stated users' IoT awareness affects their IoT privacy knowledge was accepted. Hypothesis 2 that stated users' IoT awareness affects their IoT security knowledge was accepted. Hypothesis 3 that stated users' IoT privacy knowledge affects their IoT trust was accepted. Hypothesis 4 that stated users' IoT security knowledge affects their IoT trust was accepted. Hypothesis 5 that stated users' IoT trust affects their continued intention to use IoT was accepted.

5.4. *Mediation*

Table 8 shows the results for hypothesis 6 that stated the mediation relationship in the research model exists between the independent and dependent variables. Results indicated the relationship between IoT awareness and IoT trust is mediated by both users' IoT privacy knowledge and users' IoT security knowledge. The relationship between IoT awareness and continued intention to use IoT is mediated by both users' IoT security knowledge and users' IoT trust.

6. Discussion

Our findings indicated that (1) IoT awareness positively influences users' knowledge of IoT privacy and security; (2) the users' knowledge of IoT privacy and security positively influences users' IoT trust; (3) the users' IoT trust positively influences continued intention to use IoT. These results have been emphasized separately in various studies, i.e., IoT awareness can increase the knowledge of privacy and security (e.g., Adjerid et al., 2018; Alasdair, 2017; Chen & Wen, 2019; Rice & Bogdanov, 2019), users' knowledge of privacy and security may ensure trust in IoT (e.g., Li et al., 2021; Russell & Van Duran, 2018; Sanfilippo et al., 2020; Yarali et al., 2017), and IoT trust can act as a vital factor in the possible continued use of IoT (e.g., Gao & Bai, 2014; Tsourela & Nerantzaki, 2020). Furthermore, we found that IoT privacy knowledge, IoT security knowledge, and IoT trust were mediating factors between IoT awareness and continued intention to use IoT. In this section, we discuss the theoretical and practical implications of these findings.

6.1. *Theoretical contributions and implications*

The findings of this study embrace several theoretical implications confirming our proposed research model. The strength of the proposed research model was confirmed. The reliability (indicator reliability and internal consistency) of the research model was confirmed. Next, the validity (convergent and discriminant) of the proposed research model was established. Subsequently, the variance inflation factor (VIF) for all the predictor constructs showed no collinearity concerns. Upon establishing the reliability and validity of the research model, the structural model was evaluated using coefficient of determination (R^2) were moderate to high values were reported for all endogenous or predictive constructs and blindfolding-based cross-validated redundancy measure (Q^2) where predictive accuracy of the structural model for all endogenous or predictive constructs suggested a well-grounded predictive relevance for the research model. These results indicate that the research

Table 7
Coefficient table.

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
AWARE -> PRIVACY	0.698	0.696	0.042	16.808	**0.000**
AWARE -> SECURITY	0.733	0.731	0.036	20.413	**0.000**
PRIVACY -> TRUST	0.142	0.141	0.075	1.894	**0.029**
SECURITY -> TRUST	0.188	0.190	0.073	2.568	**0.005**
TRUST -> INTENT	0.282	0.282	0.073	3.872	**0.000**

Table 8
Mediation.

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
AWARE -> PRIVACY -> TRUST	0.099	0.099	0.053	1.883	**0.030**
AWARE -> SECURITY -> TRUST	0.138	0.139	0.054	2.541	**0.006**
AWARE -> SECURITY -> TRUST -> INTENT	0.039	0.041	0.022	1.787	**0.037**

model is powerful enough to describe the directed dependencies among all the variables in the research model including the mediating variables.

In our proposed model, via path modeling, we found that the users' IoT awareness is significantly related to their knowledge about IoT privacy security issues. In other words, as users increase their awareness of security/privacy threats of IoT devices, their privacy and privacy knowledge also increase. We also found that the users' IoT privacy knowledge and the users' IoT security knowledge both significantly affect their IoT trust. In other words, as users become savvier about IoT privacy and security, they place more trust in their IoT devices and their service providers (i.e., they believe the IoT vendors are trustworthy, benevolent, and skillful in protecting their personal information and networks). Further, the users' IoT trust affects their continued intention of users to use IoT. In other words, users' IoT trust that their IoT service providers are trustworthy, benevolent, and skillful in protecting their personal information significantly influences users' continued intention to use IoT services.

Finally, our assertion that mediation exists between the independent and dependent variables in our research model was supported. In the research model, the relationship between IoT awareness and IoT trust is mediated by both users' IoT privacy knowledge and users' IoT security knowledge. The relationship between IoT awareness and continued intention to use IoT is mediated by both users' IoT security knowledge and Users' IoT trust.

6.2. Implications for practice

First, a major practical implication of these findings within organizations should be the careful and serious attention to providing IoT awareness and training programs. As Wilson and Hash (2003) stated "… awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers." Furthermore, an awareness and training program acts as the engine for circulating critical information that users need to safeguard their devices against threats and risks, ultimately safeguarding the organizations (Wilson & Hash, 2003). An organization's IoT awareness and training program must focus on basic education about IoT security vulnerabilities (e.g., botnet, malware, high-jacking/ransomware, rogue devices, exploitation of Internet-connected cameras and/or users' cloud service, etc.) and privacy issues (e.g., collection, secondary usage, and improper access of personal information). The critical emphasis must be on users' understanding of how to avoid these threats and risks by changing the default password, disabling features that are not needed, installing automatic patches and updates, using multi-factor authentication, update default settings, never use public Wi-Fi at work, etc. Furthermore, a critical element of an IoT awareness and training program within organizations is the IoT policy compliance that includes appropriate rules of behavior for all users. The IoT policy compliance can be the major influencer in safeguarding organizations against IoT security and privacy threats and risks. The IoT policy compliance must be constantly communicated to all users within organizations.

Second, in the proposed research model, we found that the relationship between IoT awareness and IoT trust is mediated by both users' IoT privacy knowledge and users' IoT security knowledge. Additionally, the relationship between IoT awareness and continued intention to use IoT is mediated by both users' IoT security knowledge and users' IoT trust. Therefore, to elevate users' IoT trust and increase users' continued intention to use IoT, we recommend that an organization's IoT awareness and training program should include and emphasize these mediating variables within the awareness programs.

Third, we believe that conducting IoT awareness and training for users within organizations is not adequate to completely safeguard the organizations' assets. Therefore, we suggest that an IoT awareness and training program must be embedded within the culture of an organization. Threats, risks, vulnerabilities of IoT must be instilled with all users, including the management at all levels. They must be constantly reminded that the protection against threats, risks, and vulnerabilities of IoT is the responsibility of everyone within the organization. A leadership-driven IoT awareness and training program documents policies and compliances; provides regular and routine training, and encourages users to report threat incidents. Increased knowledge would lead to better strategies and confidence in addressing issues, leading to trust. This combination of knowledge and confidence translates to trust and the continued intention to use IoT. As such, organizations that provide IoT awareness can help their employees become aware of the IoT threats, risks, and vulnerabilities. Therefore, give them the knowledge to build skills and confidence to safely use IoT to protect the organizations' assets against threats, risks, and vulnerabilities.

6.3. Limitation, and future direction

This study has limitations that may constrain the generalizability of the results. First, the survey used in the study was a traditional statement-based method survey. While this method is used extensively, we believe that using a scenario-based method approach to measure prospective behaviors can be considered to validate the present study's results. Second, a sample of convenience was used to collect the data for this study. Future research may consider using a random sample to validate the results of the present study. Finally, future research may consider including other variables/constructs, i.e., usability and utility factors in the model that may affect the continued use of IoT.

7. Conclusions

Via path modeling, this study proposed a model with five constructs to conclude that IoT awareness can positively influence users' IoT privacy and security knowledge. This increase in users' IoT privacy and security knowledge can positively influence users' IoT trust. Subsequently, the users' IoT trust can influence continued intention to use IoT. In addition, IoT privacy knowledge, IoT security knowledge, and IoT trust were found to be the mediating variables in the proposed model. In other words, IoT privacy knowledge mediated the relationship between IoT awareness and IoT trust. Furthermore, IoT security knowledge mediated the relationship between IoT awareness and trust. Moreover, IoT security knowledge and IoT trust were mediators between awareness and intention to use IoT. These findings can guide organizations to provide careful attention to these variables when developing, designing, and implementing IoT awareness and training programs that educate users to safeguard the organizations' assets against threats, risks, and vulnerabilities. This research has contributed to building a better understanding of how IoT awareness can play a significant role in IoT privacy and security knowledge that in turn affecting the IoT trust and consequently leading to continued use of IoT.

CRediT authorship contribution statement

Alex Koohang: Conceptualization, Methodology, Formal analysis, Resources, Writing – original draft, Writing – review & editing, Visualization, Supervision. **Carol Springer Sargent:** Conceptualization, Investigation, Resources, Writing – original draft, Writing – review & editing, Visualization. **Jeretta Horn Nord:** Conceptualization, Investigation, Resources, Writing – review & editing, Visualization. **Joanna Paliszkiewicz:** Conceptualization, Investigation, Resources, Writing – Review & editing, Visualization.

Declaration of Competing Interest

There is no financial and personal relationships with other people or organizations that could inappropriately influence (bias) our work.

Appendix A. (Measures)

IoT Awareness (AWARE).

1. My company makes me aware of constantly evolving security/privacy threats and risks of IoT.
2. My company provides me with basics awareness of security/privacy threats and risks of IoT.
3. My company provides me with an understanding of what generates security/privacy threats and risks of IoT.

Source: Designed for the present study.

IoT Privacy Knowledge (PRIVACY).

1. I know that IoT service providers may be collecting personal information about me.
2. I know that IoT service providers would share my stored personal information in their databases with other companies without my authorization.
3. I know that IoT service providers' databases that contain my personal information may not be protected from unauthorized access.

Source: Adapted and modified for IoT privacy knowledge from Koohang et al. (2018).

IoT Security Knowledge (SECURITY).

1. I know about IoT security vulnerabilities stemming from IoT service providers (i.e., botnet, malware, highjacking/ransomware, rogue devices, etc.) that may give attackers unauthorized access to the IoT devices I use.
2. I know about IoT-based data breaches stemming from IoT service providers (i.e., exploitation of Internet-connected cameras and/or users' cloud service, etc.) allowing an attacker access to potentially sensitive data or other valuable information.
3. I know about the lack of IoT service providers' regular patches and updates to the IoT devices I use.

Source: Adapted from Zhang and Gupta (2018) *and modified for IoT security knowledge*.

IoT Trust (TRUST).

1. The IoT service providers that provide products and applications I use would be trustworthy to protect me against security/privacy threats and risks.
2. The IoT service providers that provide products and applications I use would keep my best interests and well-being in mind to protect me against security/privacy threats and risks.
3. The IoT service providers that provide products and applications I use are skilled enough to protect me against security/privacy threats and risks.

Source: Adapted from Koohang et al. (2020) *and modified for IoT trust*.

Continued Intention to Use IoT (INTENT).

1. I intend to continue using IoT services.
2. I intend to keep using IoT services in the future.

Source: Adapted & Modified from Hsu and C.-L (2016a).

References

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly, 42*(2), 465–A465. https://doi.org/10.25300/MISQ/2018/14316

Alaiad, A., & Zhou, L. (2017). Patients' adoption of WSN-Based Smart Home Healthcare Systems: An Integrated Model of Facilitators and Barriers. *IEEE Transactions on Professional Communication, 60*(1), 4–23. https://doi.org/10.1109/TPC.2016.2632822

Alasdair, G. (2017). *IoT Security Issues* (1st ed.). De=G Press ⟨https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=nlebk&AN=1630323&site=ehost-live&custid=ns235467⟩.

Almusaylim, Z. A., & Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness Internet of Things (IoT). *Wireless Networks, 25*(6), 3193–3204. https://doi.org/10.1007/s11276-018-1712-5

Alshehri, M. D., & Hussain, F. K. (2019). A fuzzy security protocol for trust management in the Internet of Things (Fuzzy-IoT). *Computing, 101*(7), 791–818. https://doi.org/10.1007/s00607-018-0685-7

Ando, R., Shima, S., & Takemure, T. (2016). Analysis of privacy and security affecting the intention of use in personal data collection in an IoT environment. *IEICE Transactions on Information and Systems, E99-D*(8), 1974–1981. https://doi.org/10.1587/transinf.2015INI0002

Arfi, W. B., Nasr, I. B., Kondrateva, G., & Hikkerova, L. (2021). The role of trust in intention to use the IoT in eHealth: Application of the modified UTAUT in a consumer context. *Technological Forecasting and Social Change, 167*, 1. https://doi.org/10.1016/j.techfore.2021.120688

Asad, M., Moustafa, A., & Yu, C. (2020). A critical evaluation of privacy and security threats in federated learning. *Sensors, 20*(24), 7182. https://doi.org/10.3390/s20247182

Attarian, R., & Hashemi, S. (2021). An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. *Computer Networks, 190*, Article 107976. https://doi.org/10.1016/j.comnet.2021.107976

Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks, 192*, Article 108040. https://doi.org/10.1016/j.comnet.2021.108040

Bansal, M., Chana, I., & Clarke, S. (2020). A survey on IoT big data: Current status, 13 V's challenges, and future directions. *ACM Computing Surveys, 53*(6), 1–59. https://doi.org/10.1145/3419634

Baranwal, G., Singh, M., & Vidyarthi, D. P. (2020). A framework for IoT service selection. *Journal of Supercomputing, 76*(4), 2777–2814. https://doi.org/10.1007/s11227-019-03076-1

Becerra, E. P., & Korgaonkar, P. K. (2011). Effects of trust beliefs on consumers' online intentions. *European Journal of Marketing, 45*(6), 936–962. https://doi.org/10.1108/03090561111119921

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: A literature review. *International Journal of Production Research, 57* (15–16), 4719–4742.

Bica, I., Chifor, B.-C., Arseni, Ș.-C., & Matei, I. (2019). Multi-layer IoT security framework for ambient intelligence environments. *Sensors, 19*(18), 4038. https://doi.org/10.3390/s19184038

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management, 51*, Article 101952.

Burhan, M., Rehman, R. A., Khan, B., & Byung-Seo, K. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors, 18*(9), 2796. https://doi.org/10.3390/s18092796

Chatterjee, S., Kar, A. K., & Dwivedi, Y. K. (2021). Intention to use IoT by aged Indian consumers. *Journal of Computer Information Systems*, 1–12. https://doi.org/10.1080/08874417.2021.1873080

Carrión, G., Nitzl, C., & Roldán, J. (2017). Mediation analyses in partial least squares structural equation modeling: Guidelines and empirical examples. *Partial least squares path modeling* (pp. 173–195). Cham: Springer.

Celik, Z. B., Fernandes, E., Pauley, E., Gang, T. A. N., & McDaniel, P. (2019). Program analysis of commodity IoT Applications for security and privacy: challenges and opportunities. *ACM Computing Surveys, 52*(4), 1–30. https://doi.org/10.1145/3333501

Chen, Y.-N. K., & Wen, C.-H. R. (2019). Taiwanese university students'smartphone use and the privacy paradox. *Uso del teléfono inteligente en universitarios taiwaneses y la paradoja de laprivacidad*, 27 (60), 61– 69. Retrieved from: ⟨https://doi.org/10.3916/C60-2019-06⟩.

Duan, R., & Guo, L. (2021). Application of blockchain for internet of things: A bibliometric analysis. *Mathematical Problems in Engineering*, 1–16. https://doi.org/10.1155/2021/5547530

Dubno, D. (2017). Is someone going to hack my lightbulb? *Popular Mechanics*, 77.

Economist. (2019). Hack the planet. *Economist, 432*, 11–13. ⟨https://www.economist.com/technology-quarterly/2019/09/12/a-connected-world-will-be-a-playground-for-hackers⟩.

Fang, J., & Feng, T. (2021). Group signature with time-bound keys and unforgeability of expiry time for smart cities. *EURASIP Journal on Wireless Communications & Networking, 2021*(1), 1–22. https://doi.org/10.1186/s13638-021-01948-w

Ferraris, D., & Fernandez-Gago, C. (2020). TrUStAPIS: A trust requirements elicitation method for IoT. *International Journal of Information Security, 19*(1), 111–127. https://doi.org/10.1007/s10207-019-00438-x

Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics, 26*, 211–231.

Ghosh, A., Edwards, D. J., & Hosseini, M. R. (2021). Patterns and trends in Internet of Things (IoT) research: Future applications in the construction industry. *Engineering Construction & Architectural Management, 28*(2), 457–481. https://doi.org/10.1108/ECAM-04-2020-0271

Guo, J., Chen, R., & Tsai, J. J. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications, 97*, 1–14.

Ha, N. T., Huong, N. T. L., Nguyen, T. P. L., & GNguyen, T. D. (2019). The effect of trust on consumers' online purchase intention: An integration of TAM and TPB. *Management Science, 9*(9), 1451–1460. https://doi.org/10.5267/j.msl.2019.5.006

Hair, J., Risher, J., Sarstedt, M., & Ringle, C. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hamdani, S. W. A., Khan, A. W., Iltaf, N., Bangash, J. I., Bangash, Y. A., & Khan, A. (2021). Dynamic distributed trust management scheme for the Internet of Things. *Turkish Journal of Electrical Engineering & Computer Sciences, 29*(2), 796–815. https://doi.org/10.3906/elk-2003-5

Hsu, C.-L., & Lin, J. C.-C. (2016a). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior, 62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Hsu, C.-L., & Lin, J. C.-C. (2016b). Factors affecting the adoption of cloud services in enterprises. *Information Systems and eBusiness Management, 14*(4), 791–822. https://doi.org/10.1007/s10257-015-0300-9

Hsu, C.-L., & Lin, J. C.-C. (2018). Exploring factors affecting the adoption of internet of things services. *Journal of Computer Information Systems, 58*(1), 49–57. https://doi.org/10.1080/08874417.2016.1186524

Huang, X., Craig, P., Lin, H., & Yan, Z. (2016). SecIoT: A security framework for the internet of things. *Security and Communication Networks, 9*(16), 3083–3094.

ISACA (2019). *In time for data privacy day, new resources provide enterprises with tools for navigating and addressing privacy challenges and regulations*. Retrieved from: ⟨https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/in-time-for-data-privacy-day-new-resources-provide-enterprises-with-tools-for-navigating-and⟩ (Accessed 9 March 2021).

Jayashankar, P., Nilakanta, S., Johnston, W. J., Gill, P., & Burres, R. (2018). IoT adoption in agriculture: the role of trust, perceived value and risk. *Journal of Business & Industrial Marketing, 33*(6), 804–821.

Jiang, Q., Zhang, X., Zhang, N., Tian, Y., Ma, X., & Ma, J. (2021). Three-factor authentication protocol using physical unclonable function for IoV. *Computer Communications, 173*, 45–55. https://doi.org/10.1016/j.comcom.2021.03.022

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PLoS One, 15* (1), 1–21. https://doi.org/10.1371/journal.pone.0227800

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy Valuation, transparency features, and service personalization. *Journal of Management Information Systems, 34*(2), 369–400. https://doi.org/10.1080/07421222.2017.1334467

Kassab, M., DeFranco, J., & Laplante, P. (2020). A systematic literature review on Internet of Things in education: Benefits and challenges. *Journal of Computer Assisted Learning, 36*(2), 115–127.

Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The internet of things: Impact and implications for health care delivery. *Journal of Medical Internet Research, 22*(11), 20135. https://doi.org/10.2196/20135

Kerner, S. M. (2017). The internet of evil things being fueled by Mirai Botnet. *eWeek*, 1-1 ⟨https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=fth&AN=121495567&site=ehost-live&custid=ns235467⟩.

Koohang, A., Nowak, A., Paliszkiewicz, J., & Nord, J. (2020). Information security policy compliance: Leadership, trust, role values, and awareness. *Journal of Computer Information Systems, 60*(1), 1–8.

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management & Data Systems, 118*(6), 1209–1228.

Lee, H. (2020). Home IoT resistance: Extended privacy and vulnerability perspective. *Telematics & Informatics, 49*. https://doi.org/10.1016/j.tele.2020.101377

Lellis, C. (2020). *Mobile devices in the workplace: 40 statistics you should know in 2021*. Retrieved from ⟨https://www.perillon.com/blog/mobile-statistics-devices-at-work⟩.

Li, X., Wang, Z., Leung, V. C. M., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks: A survey and outlook. *ACM Computing Surveys, 54* (3), 1–38. https://doi.org/10.1145/3446373

Li, Y., & Shin, B.-S. (2018). Privacy-aware task data management using TPR*-Tree for trajectory-based crowdsourcing. *Journal of Supercomputing, 74*(12), 6976–6987. https://doi.org/10.1007/s11227-018-2486-3

Lin, H. (2011). An empirical investigation of mobile banking adoption: the effect of innovation attributes and knowledge-based trust. *International Journal of Information Management, 3*(31), 252–260.

Ling, K. C., Chai, L. T., & Piew, T. H. (2010). The effects of shopping orientations, online trust and prior online purchase experience towards customers' online purchase intention. *International Business Research, 3*(3), 63–76.

Lundqvist, B. (2019). Cloud services as the ultimate gate(keeper). *Journal of Antitrust Enforcement, 7*(2), 220–248. https://doi.org/10.1093/jaenfo/jny013

Mani, Z., & Chouk, I. (2017). Drivers of consumers' resistance to smart products. *Journal of Marketing Management, 33*(1/2), 76–97. https://doi.org/10.1080/0267257X.2016.1245212

Marketwired. (2015). CyberTECH sponsoring "Data Privacy Day 2015: Securing the Internet of Things" National seminar. *Marketwired*.

Mattern, F., & Floerkemeier, C. (2010). From the internet of computers to the internet of things. In K. Sachs, I. Petrov, & P. Guerrero (Eds.), *From active data management to event-based systems and more, 6462* pp. 242–259). Berlin/Heidelberg, Germany: Springer.

Newswire. (2015). *Internet of things (IoT): Technology, outlook and significance*. USA: PR Newswire.

Newswire. (2016a). *Half of Americans discouraged from purchasing "Internet of Things" devices due to cybersecurity concerns*. USA: PR Newswire.

Newswire. (2016b). *Leading IoT vendors promote privacy awareness with privacynq brief*. USA: PR Newswire. ⟨https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=bwh&AN=201601280835PR.NEWS.USPR.PH09275&site=ehost-live&custid=ns235467⟩.

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The internet of things: Review and theoretical framework. *Expert Systems with Applications, 133*, 97–108. https://doi.org/10.1016/j.eswa.2019.05.014

Oke, A. E., Arowoiya, V. A., & Akomolafe, O. T. (2020). Influence of the Internet of Things' application on construction project performance. *International Journal of Construction Management*, 1–11. https://doi.org/10.1080/15623599.2020.1807731

Osmonbekov, T., & Johnston, W. J. (2018). Adoption of the Internet of Things technologies in business procurement: Impact on organizational buying behavior. *Journal of Business & Industrial Marketing, 33*(6), 781–791. https://doi.org/10.1108/JBIM-10-2015-0190

Pitichat, T. (2013). Smartphones in the workplace: Changing organizational behavior, transforming the future. *LUX: A Journal of Transdisciplinary Writing and Research from Claremont Graduate University, 3*(1), 13-10.

Polat, H., & Du, W. (2005). Privacy-preserving collaborative filtering. *International Journal of Electronic Commerce, 9*(4), 9–35. https://doi.org/10.1080/10864415.2003.11044341

Ranjan, S., Jha, V., & Pal, P. (2017). Application of emerging technologies in ERP implementation in Indian manufacturing enterprises: An exploratory analysis of strategic benefits. *International Journal of Advanced Manufacturing Technology, 88* (1–4), 369–380. https://doi.org/10.1007/s00170-016-8770-6

Rashid, M. R. A., Conzon, D., Tao, X., & Ferrera, E. (2020). Privacy awareness for IoT platforms: BRAIN-IoT approach. In R. Hernández, J. Luis, & A. Skármeta (Eds.), *Security and privacy in the internet of things: Challenges and solutions* (pp. 24–42). IOS Press.

Ren, H., Li, H., Dai, Y., Yang, K., & Lin, X. (2018). Querying in internet of things with privacy preserving: challenges, solutions and opportunities. *IEEE Network, 32*(6), 144–151. https://doi.org/10.1109/MNET.2018.1700374

Rice, M. D., & Bogdanov, E. (2019). Privacy in doubt: An empirical investigation of canadians' knowledge of corporate data collection and usage practices. *Canadian Journal of Administrative Sciences, 36*(2), 163–176. https://doi.org/10.1002/cjas.1494

Ringle, C., Wende, S., & Will, A. (2005). *SmartPLS 3.0*. Hamburg: SmartPLS. ⟨www.smartpls.de⟩.

Russell, B., & Van Duran, D. (2018). *Practical Internet of Things security: Design a security framework for an Internet connected ecosystem* (2nd ed.). Packt Publishing.

Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., & Egelman, S. (2020). Disaster privacy/privacy disaster. *Journal of the Association for Information Science & Technology, 71*(9), 1002–1014. https://doi.org/10.1002/asi.24353

Schneier, B. (2017). BOTNETS of things. *Mitosz Technology Review, 120*(2), 88–91. ⟨https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=rgm&AN=121426366&site=ehost-live&custid=ns235467⟩.

Sharma, M., Joshi, S., Kannan, D., Govindan, K., Singh, R., & Purohit, H. C. (2020). Internet of Things (IoT) adoption barriers of smart cities' waste management: An Indian context. *Journal of Cleaner Production, 270*, Article 122047. https://doi.org/10.1016/j.jclepro.2020.122047

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Network, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Song, L., Ju, X., Zhu, Z., & Li, M. (2021). An access control model for the Internet of Things based on zero-knowledge token and blockchain. *EURASIP Journal on Wireless Communications & Networking, 2021*(1), 1–20. https://doi.org/10.1186/s13638-021-01986-4

Tikhvinskiy, V., & Bochechka, G. (2017). Quality of service in the 5G network. In A. Yarali (Ed.), *5G mobile: From research and innovations to deployment aspects*. Nova Science Publishers, Inc.

Tinamas, P., & Natwichai, J. (2020). Issues in privacy preservation for re-publishable data. In F. Xhafa, & A. K. Sangaiah (Eds.), *Advances in edge computing: Massive parallel processing and applications*. IOS Press.

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: Challenges, issues and solutions at different IoT layers. *Journal of Supercomputing*, 1–37. https://doi.org/10.1007/s11227-021-03825-1

Tsourela, M., & Nerantzaki, D. M. (2020). An Internet of Things (IoT) Acceptance Model. Assessing consumer's behavior toward IoT products and applications. *Future Internet, 12*(11), 191.

Urrico, R. O. Y. (2018). Understanding the rewards, cyber risks of IoT devices. *Credit Union Times, 29*(4), 6. ⟨https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=bth&AN=127750443&site=ehost-live&custid=ns235467⟩.

Vignau, B., Khoury, R., Hallé, S., & Hamou-Lhadj, A. (2021). The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives. *Journal of Systems Architecture, 116*. https://doi.org/10.1016/j.sysarc.2021.102143

Waheed, N., Xiangjian, H. E., Ikram, M., Usman, M., & Hashmi, S. S. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. *ACM Computing Surveys, 53*(6), 1–37. https://doi.org/10.1145/3417987

Wang, E. S.-T. (2019). Effects of brand awareness and social norms on user-perceived cyber privacy risk. *International Journal of Electronic Commerce, 23*(2), 272–293. https://doi.org/10.1080/10864415.2018.1564553

Wang, Y., Yan, Z., Feng, W., & Liu, S. (2020). Privacy protection in mobile crowd sensing: a survey. *World Wide Web, 23*(1), 421–452. https://doi.org/10.1007/s11280-019-00745-2

Weber, M., & Podnar Žarko, I. (2019). A regulatory view on smart city services. *Sensors, 19*(2), 415. https://doi.org/10.3390/s19020415

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication, 800*(50), 1–39.

Wirtz, B. W., Weyerer, J. C., & Schichtel, F. T. (2019). An integrative public IoT framework for smart government. *Government Information Quarterly, 36*(2), 333–345. https://doi.org/10.1016/j.giq.2018.07.001

Yarali, A., Yedla, R., Almalki, S., Covey, K., & Almohanna, M. (2017). Security, privacy and trust in 5G wireless mobile communications. In A. Yarali (Ed.), *5G mobile: From research and innovations to deployment aspects* (pp. 147–162). Nova Science Publishers, Inc.

Zhang, Q., Zhong, H., Shi, W., & Liu, L. (2021). A trusted and collaborative framework for deep learning in IoT. *Computer Networks, 193*, Article 108055. https://doi.org/10.1016/j.comnet.2021.108055

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: overview and new direction. *Future Generation Computer Systems, 86*, 914–925.