Contents lists available at ScienceDirect

Technological Forecasting & Social Change

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

Frontline healthcare providers' behavioural intention to Internet of Things (IoT)-enabled healthcare applications: A gender-based, cross-generational study

Mansour Alraja [*]

Department of Management Information Systems, Dhofar University, Salalah, Oman

ARTICLE INFO

Keywords:
Security and privacy
Trust
Risk perception
Frontline healthcare providers
Internet of things
Gender

ABSTRACT

There are numerous risks associated with the interconnection of healthcare provision and the Internet of Things (IoT), with its sensory capabilities shown to reduce confidence in novel technology due to fears of a loss of privacy. There exists a clear omission in the extant literature—consideration of gender differences in Frontline Healthcare Providers' (FHP) behavioural intentions—which this work aims to address through the analysis of IoT-enabled healthcare applications' (HAs) behavioural intentions in multicultural and bi-generational (Gen X, Y) context. Essentially, analysing gender and generational differences in relation to the variables (privacy, security and trust that influence risk perception; the latter alongside attitude and perceived behavioural control potentially affect the intention) affecting FHPs' BI towards IoT enabled HAs. A novel model is presented herein, which combines Planned Behaviour (TPB), Privacy Calculus (PCT), and the trust-risk framework. Questionnaire methodology (n = 401) was applied to both generations under consideration, data was assessed using Partial Least Squares Multi-Group Analysis (PLS-MGA), which showed gender differences in Gen Y, but there was little evidence to suggest that risk perception affects any of the cohort's behavioural intention towards the use of IoT-enabled HA, which in turn should help guide both future institutional policy and application development .

1. Introduction

Advances in network technologies, combined with mass production of smart devices equipped with sensors with continuous, bidirectional transmission, and the advent of cloud computing have been the primary drivers behind IoT development and implementation in big data driven infrastructural control (Hassan et al., 2018; Li et al., 2020; Rafique et al., 2020; Razzak et al., 2020). However, the security problems inherent in the wider internet itself remain prevalent in IoT. In truth, each element in IoT's tri-layer structure—perception, transport, and application—requires individual consideration in that respect (Tewari and Gupta, 2020). IoT is now commonplace in modern society, often appearing in the food supply chain, logistics, mining, computing, and healthcare sectors (Pang et al., 2015; Yildirim and Ali-Eldin, 2019). Particularly in the case of the latter, the drive for service improvement has resulted in a broad body of literature considering this advance (Asif-Ur-Rahman et al., 2019; Syed et al., 2019).

The interconnected nature of the IoT enabled healthcare model (Tewari and Gupta, 2020) contains a multitude of risks relating to privacy, security and loss of trust. Limitations on the computational ability of this model means that conventional measures used to tackle security and privacy concerns often cannot be applied (Li et al., 2020), leading to the development of a concept known as the Internet of Medical Things, wherein patient data confidentiality without loss of functionality is held paramount (Li et al., 2020).

The majority of past research has focused on technological issues surrounding IoT, with little attention paid to actual take-up. Notwithstanding this, previous authors have considered this take-up, across a variety of sectors, using the technology acceptance model (Gao and Bai, 2014); behavioural reasoning theory (Pillai and Sivathanu, 2020); external pressure and cost-benefit perception (Tu, 2018); employee intention analysis (albeit with limited usefulness due to poor experimental design and a small, non-representative sample) (Yildirim and Ali-Eldin, 2019); a combination of unified theory of acceptance and use of technology, financial costing, and risk perception (although they concluded that cost and age are critical factors, its validity is again limited by choice of sample, and lack of consideration of other factors such as trust, privacy, or security) (Ben Arfi et al., 2020); synthesis of

[*] Corresponding author.
E-mail address: malraja@du.edu.om.

https://doi.org/10.1016/j.techfore.2021.121256
Received 8 January 2021; Received in revised form 20 September 2021; Accepted 27 September 2021
Available online 6 October 2021

parts of both technology acceptance model (with cost, privacy, self-efficacy) and of innovation diffusion theory (trial ability, image, and compatibility) in the medical sector (generalisation of the results presented is unwise due to a combination of a small (n = 124), localised sample and the single factor considered—privacy) (Alhasan et al., 2020). Although some conclusions can be drawn from these works, and may assist in managerial design in their respective sectors, the primary revelation is that their limitations provide the foundation for this work to address.

Whilst IoT-healthcare synthesis allows for contemporary, continuous monitoring and tracking of system components such as medicines, devices, doctors, and patients, and the ability to rapidly share data between them using smart software (Plaza et al., 2011), some privacy and security issues remain (Tewari and Gupta, 2020).

The review above shows that the primary focus has been on technological aspects, with comparatively little attention paid to end user readiness, intention, or sector specific application. However, due to the relative immaturity of the sector as a whole, it is vital to consider a broader, multiscale, multisector perspective if maturity is ever to be attained.

There are clear gender divides governing acceptance and use of technology (Alraja et al., 2019; Ameen et al., 2020; Nami and Vaezi, 2018; Tarhini et al., 2017), and thus it seems apt to consider these divides during this study of employees' behavioural intention (BI) toward using IoT-enabled HAs.

Approximately half of the global workforce are female, and thus women are considered vital contributors to the global economy (Ameen et al., 2020; Madichie and Gallant, 2012). This paper will focus on females' contributions in Omani context, and thus it is necessary to provide a population overview. Wage equality in Oman sits at 5.68 out of 7, yet women hold only a quarter of total professional jobs. A majority (55.6%) attended tertiary education (compared with only 26.4% of men). At 6.98%, women are over three times as likely to possess health and welfare skills, while the percentage with ICT skills (17.0%) also surpasses the male population (9.24%) (World Economic Forum, 2020). There is little published work considering the intersectional nature of gender differences and multiculturalism and how they affect employee's BI toward IoT-enabled HAs. The international outlook of modern companies means it is imperative that they consider these interrelations in the development of training and recruitment policies. Oman provides the ideal case study for these considerations due to the high proportion (42.5%. 1.43m) of expatriates working in the country NCSI (2020).

This study provides a valuable contribution to literature by considering how gender differences affect employees' BI toward IoT-enabled HAs in healthcare organisations by proposing a novel model for IoT adoption—comprising a synthesis of TPB Ajzen (1991) PCT (Culnan and Armstrong, 1999) and the trust risk framework (Mayer et al., 1995a)—which aims to reveal both gender (male/female) and generational dissimilarities (Gen X, born 1965–80; Gen Y, born 1981–96). As a means of increasing the level of generalisability, consideration is also given to the effects of multiculturalism on FHPs' behavioural intentions. The real world value of this study lies in its applicability to improving the efficacy of managerial strategies in global corporations by understanding the benefits and drawbacks of possessing a multicultural, multi-gendered, cross generational workforce and increasing awareness of how their reaction to novel IoT technologies affects overall perceptions of security, trust, and privacy risks.

The upcoming sections provides a focused literature review, a discussion of relevant theory, and presents hypotheses. This is followed by methodology and results sections, after which a contextualised discussion of their implications in relation to the literature is given, with special consideration made for both limitations and future work proposals.

2. Theoretical background

2.1. Gender and IoT

The extant body of information systems literature has pondered the existence of a gender divide in novel technology adoption, with several authors concluding that sex-role stereotyping, technological positivity and self-efficacy are more prevalent in the male population (Cai et al., 2017; Compeau and Higgins, 1995). The literature provides numerous examples of gender split with respect to IoT security, wherein women are typically more compliant with protocols (Anwar et al., 2017; Ifinedo, 2014), whereas men categorise e-shopping and, in general, cybersecurity as comparatively low risk activities (Ameen et al., 2021; Garbarino and Strahilevitz, 2004; Mamonov and Benbunan-Fich, 2018). As Gen Y are considered to be digital natives, they tend not to see these novel technologies as anything but ordinary tools in their everyday existence, with little consideration given to security concerns associated with them, with women instead choosing to worry more about product reliability and a lack of familiarity (Yang et al., 2018). This contrasts well with Gen X, who typically have a larger gender divide around these attributes (Albert et al., 2019).

The theory of planned behaviour has been extended (Cassioli et al., 2020) to include the moderating effects of gender, for example on workplace technological uptake (Morris et al., 2005), green restaurant attendance Moon (2021), and entrepreneurial intention (Maes et al., 2014), with the latter showing that while men prioritise achievement, women favour balance.

The foundation for this study lies in that fact that comparatively few studies have considered IoT adoption intention in general, with no previous investigations exploring how this acceptance is mediated by cross-generational female specific attitudes, the intersection of gender difference and multiculturalism, or the gender-generation divide.

2.2. IoT Security, privacy, risk, and trust in healthcare

Alongside numerous other innovative technologies, the Internet of Things (IoTs) is a foremost contemporary technological innovation (Wang et al., 2014). It is deemed to be a hot research topic that has attracted academics' focus and investigation of it, being implemented across various contexts and fields (Rochwerger et al., 2009). The IoT, similar to other smart technologies, has been adopted and involved in the main processes of numerous industries, including the healthcare industry. This industry deals with a tremendous amount of complex records that must be stored without duplication, retrieved swiftly without delay or any mistakes, while also being shared with patients via a secure medium so as to prevent any criminal risks, thus safeguarding patients' privacy (Rubinstein, 2013). Within the health industry, general Technology, as well as Industry 4.0 technologies specifically (for example, IoT), have transformed the means of providing traditional health services (Chen et al., 2014). This potentially justifies the extensive applied research that uses IoT as a means of interconnecting medical resources, in addition to providing patients with effective and reliable e-healthcare services (Sun et al., 2016). Regardless, IoT in the healthcare industry may provide a solution for integrating the electronic medical records of all hospitals' information systems, thus helping to mitigate the challenges associated with sharing patients' healthcare data across different hospitals and medical centres. Accordingly, medical professionals (for instance doctors) will have the ability to view each patient's medical history, thus aiding their provision of improved treatment (Lv et al., 2017). More specifically, the healthcare industry is in urgent need of adopting and implementing smart technologies (for example, the IoT) during crises, such as the current situation with the COVID-19 pandemic. This is because they can be expected to help with providing substantial remote assistance to a tremendous number of affected people, who the health system have been unable to accommodate during this pandemic (Fosso Wamba et al., 2015).

Medical subjects are often worried about the security and confidentiality of their data, and the risk associated with leaks thereof (Ancker et al., 2013; Perera et al., 2011; Win, 2005). This is of interest to IoT development, in that while the preparation phase can be assuredly secure, online data transfer is open to many forms of misuse (Table 1-a) (Yao et al., 2020).

Multiple data storage problems have been associated with the increase in IoT implementation, and as few tools have been developed specifically for this purpose, insufficient semantic annotations are available, and thus specific concepts and models must be created soon (Barnaghi et al., 2012; Jin et al., 2014; Li et al., 2011; Tewari and Gupta, 2020). While cloud computing is the ideal site for IoT development, there are serious concerns with its data handling strategies, which must be standardised and appropriately constrained if security is to be assured (Chang et al., 2014; Rochwerger et al., 2009; Wang et al., 2014). The number of interconnected sensors operating in the IoT environment is anticipated to pass the trillion mark within the decade, yet it remains apparent that the vast majority of the data accumulated will be of little value due to a lack of standardisation (Chen et al., 2014; Fosso Wamba et al., 2015; Lv et al., 2017; Rubinstein, 2013; Sun et al., 2016). However, much of the current academic focus has been on issues surrounding trust—how best to ensure data security and legislative compliance while still reliably providing all users with an appropriate level of detail (Bao and Chen, 2012; Nitti et al., 2012; Yan et al., 2014).

Table 1
-a examples of online attacks in healthcare sector (1989-2019)

Organization/ field	Type of attack	Number of affected users	Date
Becker's Hospital	Ransomeware attack (AIDS Trojan)	20,000 floppy disks	1989
HealthNet	Identity Theft/ Hacked	531,400 patients records	2009
Lincoln Medical and Mental Health Center	AVIMEdInc attack.	180,111patients	2010
Memorial Healthcare System	TRICARE	4.9 million medical records had lost	2010
South Carolina's US Medicaid	Hacking	780,000 medical data of users	2012
Advocate Medical Group	Data stolen	medical data of about 4 million users	2013
Crescent Health Inc	Data stolen	medical data of 100,000 users	2013
Community Health Systems	Hacking and identity theft	4.5 users	2014
Anthem Inc	Identity Theft/ Hacked	80 million users	2015
CareFirst BlueCross Blue Shield-Maryland	Hacked/Identity Theft	100,000 users	2015
Medical Informatics Engineering	Hacked/Identity Theft	3.9 million records	2015
Premera	Hacked/Identity Theft	11 million records	2015
UCLA Medical Center, Santa Monica	Hacked/Identity Theft	4.5 million records	2015
21st Century Oncology	Hacked/breached	2.2 million records	2016
Apple Health Medicaid	Hacked/breached	Records of 91,000 users	2016
Inuvik hospital	Inside-job attack	6,700 users	2016
Banner health	Hacked	many users	2016
Grozio Chirurgija	Hacked	healthcare data of 25,000 users	2017
multi places	WannaCry Worm Ransomware	200,000 users	2017
Centers for Medicare and Medicaid Services	Hacked/Identity Theft	75,000 users	2018
Health Sciences Authority (Singapore)	Security/Hacked	808,000 users	2019

3. Conceptual model and hypothesis development

The Theory of Planned Behaviour (TPB), trust-risk framework, and Privacy Calculus Theory (PCT) have all previously been applied to assessment of technological take-up (Bao and Chen, 2012; Culnan and Armstrong, 1999; Hassan et al., 2018; Mayer et al., 1995b; Rafique et al., 2020; Tewari and Gupta, 2020; Yan et al., 2014).

The literature has an abundance of models adopted to investigate the area of intention to adopt new technology. These models employed various antecedents to estimate users' adoption intention. More specifically, numerous studies have incorporated two or more variables (security, privacy, trust and risk perception), with one or two technology acceptance models/theories used for estimating users' intention to adopt. For example, in the context of using social media for transactions, the trust risk-taking propensity constructs were incorporated into TAM and TPB (Hansen et al., 2018). Regarding the adoption of IoT in eHealth, the constructs of trust and perceived risk were incorporated into UTAUT (Arfi et al., 2021); to investigate intention towards mobile app installation, the security, privacy, trust and risk were all combined (Chin et al., 2018). In all of the reviewed literature, academics adopted the same approach by incorporating the constructs of security, privacy, trust, and risk perception as individual constructs rather than a model. Nevertheless, in the current study grouping, the adopted variables were linked together as follows. Firstly, the connection between the adopted variables (namely security, privacy, trust, and risk perception) and behavioural intention has been ensured in the information technology adoption literature (for more details see Table 1-b). Secondly, we grouped variables according to the previously developed theories or models. In this regard, we followed the trust-risk framework developed by Mayer, Davis and Schoorman (1995) as theoretical foundation for connecting trust and risk perception, while the privacy calculus theory (PCT) devised by Culnan and Armstrong (1999) was applied as the theoretical basis of linking privacy and security. Thirdly, TPB is acknowledged to be a flexible technique for permitting analysts to incorporate all harmonising variables, while maintaining the approach's fundamental theoretical reliability (Ajzen, 1991; Alarabiat et al., 2021; Alzubaidi et al., 2021; Holdsworth et al., 2019; Liao et al., 2007; Moon, 2021; Wu et al., 2021).

Specifically, it has evidenced reliable predictive capability in relation to BI within various research environments (Al-Debei et al., 2013). Consequently, this research has extended Ajzen's (1991) TPB by incorporating two harmonised theories/models, namely the trust-risk framework (trust, risk perception) and privacy calculus theory (security and privacy), as a foundation for forecasting frontline healthcare providers' adoption intentions in relation to IoT-based healthcare applications. To the best of the author's knowledge, no studies have analysed the causal effect of both the PCT and trust-risk framework on the BI of IoT-based healthcare applications, considering the key personal variables of attitude and PBC, particularly concerning the potential gender and generational distinctions. Additionally, TPB proposes that a person's intention may be discerned based on three key variables, namely PBC, ATT and subjective norms. Although BI refers to an individual's willingness to engage in a given behaviour, ATT defines the individual's preferred or unpreferred appraisal of the behaviour under investigation. Subjective norms concern the perceived social gravity required to attain or not to attain certain behaviour. Finally, PBC defines the extent to which an individual is able to control their engaged behaviour (Ajzen, 1991, 2001). Nevertheless, based on the nature of the provided service (healthcare services) relating to human beings' lives, we believe that the adoption decision relating to innovative methods or technologies (in our case IoT-enabled healthcare applications) should not be affected by its social gravity—which is to say, the extent to which others surrounding the users (frontline healthcare providers) will accept the mentioned behaviour—rather it should rest on expert judgement and knowledge. This accords with the research of (Hansen et al., 2018), who dropped the subjective norms from their combined model (TPB and TAM), wherein

Table 1
-b Summary Reviewed Literature on the relation between trust, risk, and intention

Path	Field	Related Constructs	Source	Underpinning Theory	Journal
Trust – Risk –Intention	Electronic commerce	• Trust • Perceived risk	(Kim et al., 2008)	valence framework	Decision Support Systems
	Organizational trust	• Trust • Risk taking	(Mayer et al., 1995a)	Developed Trust-risk framework	The Academy of Management Review
	IoT in eHealth	• Trust • Perceived risk	(Arfi et al., 2021)	UTAUT	Technological Forecasting and Social Change.
	adaptation behaviors	• Trust • Risk perception	(Azadi et al., 2019)	Integrated model based on "values–beliefs–norms" framework	Journal of Environmental Management
	Buying behavior	• Trust • Risk perception	(Hakim et al., 2020)	relevant constructs from previous studies.	Food Research International
	Mobile app installation	• Security • Privacy • Trust • Risk	(Chin et al., 2018)	Combination and extension of two previous models	International Journal of Information Management
	Use of social media for transactions	• Trust • Risk-taking propensity	(Hansen et al., 2018)	TAM and TPB	Computers in Human Behavior
	Behavior toward social media platforms	• Trust • Risk	(Wang et al., 2016)	meta-analysis	Computers in Human Behavior
	Online marketplace	• Trust • Perceived risk	(Kim and Koo, 2016)	Trust-risk framework	Computers in Human Behavior
	Mobile banking apps	• Institution-based trust • Perceived risk	(Thusi and Maduku, 2020)	UTAUT2	Computers in Human Behavior
	Online-to-Offline (O2O) as an e-commerce model	• Trust • Perceived risk	(Chen et al., 2019)	*Information systems success model*	Computers in Human Behavior
	Trust-risk relationship	• Trust • Risk	(van Riper et al., 2016)	social exchange framework	Journal of Outdoor Recreation and Tourism
	information privacy	• Perceived privacy • Trust • Privacy risk concerns	(Miltgen and Smith, 2015)	Relevant constructs from previous studies.	Information & Management
	Mobile shopping	• Trust • Risk	(Marriott and Williams, 2018)	An integrated model	Journal of Retailing and Consumer Services
	Decision-making model in electronic commerce	• Trust • Perceived risk	(Kim et al., 2008)	Valence framework	Decision Support Systems
	Mobile banking services	• Trust • Perceived risk	(Luo et al., 2010)	An integrated model	Decision Support Systems
	Cloud archiving	• Trust • Risk	(Burda and Teuteberg, 2014)	TAM	Journal of High Technology Management Research
	E-government adoption	• Trust • Perceived risk	(Bélanger and Carter, 2008)	Theory of reasoned action (TRA)	Journal of Strategic Information Systems
	Mobile devices Adoption in a high risk context	• Trust • Perceived risk	(Marett et al., 2015)	An integrated model based on adoption theories	Technology in Society
	Trust, risk perception, and COVID-19 infections	• Trust • Risk perception	(Ye and Lyu, 2020)	Multilevel analyses of combined original dataset	Social Science & Medicine
	Power grid expansion projects	• Trust • Risk expectation	(Mueller, 2020)	Combined constructs	Energy Policy
Trust –intention And/Or Risk –intention	Cloud computing	• risk analysis • perceived IT security risk • Trust	(Raut et al., 2018) And (Priyadarshinee et al., 2017)	Added risk analysis and perceived IT security risk as an extension of the Technology Organization Environment (TOE) model	Technological Forecasting and Social Change. Computers in Human Behavior
	NFC mobile payment systems	• *Perceived Risk*	(Liébana-Cabanillas et al., 2019)	TAM, DOI, and UTAUT	Technological Forecasting and Social Change
	digital personal data stores	• *Ease of use* • *Usefulness* • *Trust* • *Perceived Risk (moderator)*	(Mariani et al., 2021)	TAM	Technological Forecasting and Social Change
	Artificial intelligence	• *Perceived Risk* • *Trust*	(Hasan et al., 2020)	UTAUT2	Journal of Business Research
	electronic data exchanges	• *Perceived Risk* • *Trust*	(Nicolaou et al., 2013)	Economic exchange perspective	Decision Support Systems
		• *Perceived trust*		Combined constructs	

(*continued on next page*)

Table 1 (*continued*)

Path	Field	Related Constructs	Source	Underpinning Theory	Journal
Risk– Trust –intention	customer acceptance of internet banking	• *Perceived risk* • *Security* • *Privacy*	(Aboobucker and Bao, 2018)		Journal of High Technology Management Research
	Online payments	• *Total risk* • *Trust* • *TAM*	(Yang et al., 2015)	TAM	Computers in Human Behavior
	electronic health care records (EHCR systems)	• *Perceived risk* • *Information integrity* • *Trust*	(Ortega Egea and Román González, 2011)	TAM	Computers in Human Behavior
	near-field communication (NFC) based mobile payment	• *Risk* • *Security* • *Trust*	(Khalilzadeh et al., 2017)	UTAUT	Computers in Human Behavior
	recommendation intention	• *General* risk • *Trust*	(Al-Ansi et al., 2019)	Prospect theory	International Journal of Hospitality Managemen
	intentions to use online payment systems	• *Trust* • *Perceived risk*	(Rouibah et al., 2016)	trust model of Kim et al. (2008)	Electronic Commerce Research and Applications

they incorporated risk and trust as a means of estimating consumers' use of social media for transactions. Furthermore, empirical studies in the information technology field evidence that only PBC and attitude (as opposed to subjective norms) affect behavioural intentions, for example cyber-slacking intention (Rana et al., 2019), information security policy compliance attitude (Sommestad et al., 2015), or the use of Facebook (Raza et al., 2020). Resultantly, the decision was made to drop subjective norms in the current study.

3.1. *Theory of planned behaviour*

According to TPB, intentions are governed by three element—attitudes, perceived behavioural control, and subjective norms. The first considers a user's feelings surround a given behaviour, the second represents the difficulty of undertaking said behaviour, and the third considers how those around them will react if said behaviour is embarked upon (Ajzen, 1991). As TPB has been previously shown (Montano and Kasprzyk, 2015; Shiau and Chau, 2016) to inherently bridge the gap between literature and real life action, it is considered an ideal part of the model proposed herein (see Fig. 1).

Previous authors have found that BI is significantly influenced by both attitude and perceived behavioural control (Ajzen, 1991; Alzubaidi et al., 2021; Holdsworth et al., 2019; Knauder and Koschmieder, 2019; Moon, 2021; Olya et al., 2019; Rana et al., 2019). In this study, attitude is defined as an FHP's BI towards an IoT-enabled HA, and perceived behavioural control by their perception of its difficulty. While security compliance has previously been linked to overall intention (Raza et al., 2020; Sommestad et al., 2015), more specific details of the gender difference-HA-perceived behavioural control interplay are generally lacking in the literature, with only a few studies commenting that males show higher levels of confidence, planning, and risk taking behaviours (Hou and Elliott, 2016; Lai et al., 2008; McLaughlin et al., 2020) whereas studies of attitude have tended to report that women have greater levels of positivity towards e-commerce at large (Hou and Elliott, 2016; Riedl et al., 2010). With the exception of these studies, it is clear that a gap exists in the literature, in that little focus has been given

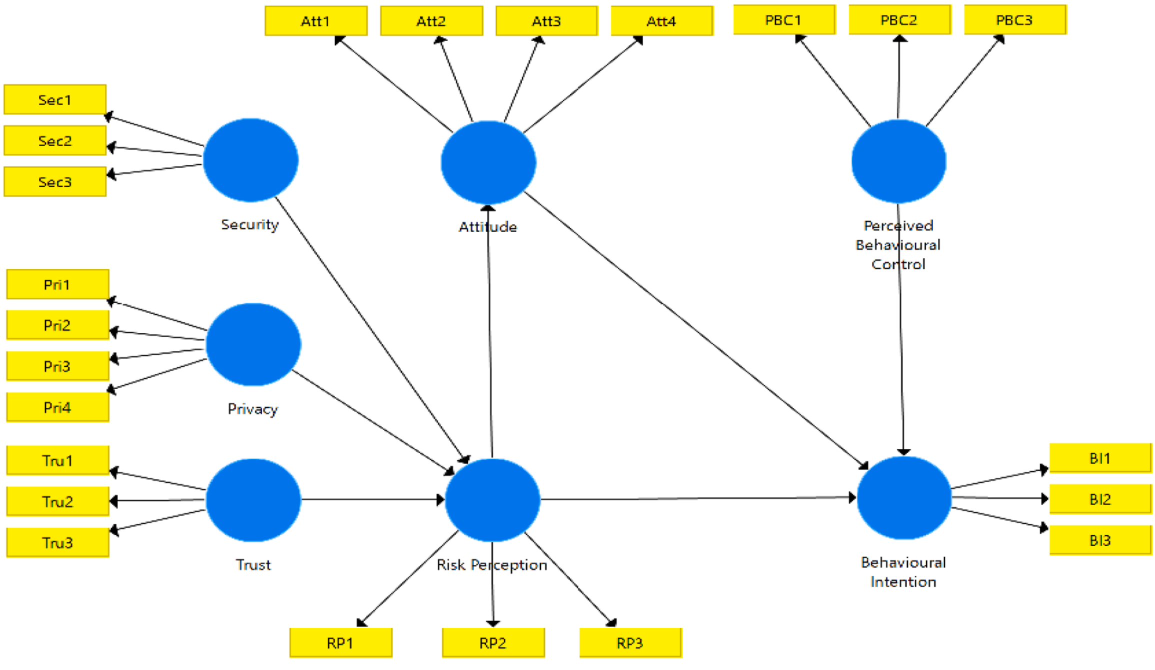

Fig. 1. research framework.

to gender divisions in FHPs' BI with respect to the implementation of IoT HAs, and thus the following hypotheses are proposed:

H1: perceived behavioural control has more significant effect on BI toward IoT-enabled HAs among female FHPs than males.
H2: Attitude has a more significant effect on BI toward IoT-enabled HAs among female FHPs than males.

3.2. Privacy calculus theory

Modern digital privacy describes user awareness of personal data collection, control, and security (Hann et al., 2007; Shah et al., 2014). It affects the BI surrounding disclosure, and can be measured using PCT (Barth and de Jong, 2017; Jozani et al., 2020; Li et al., 2011; Sun et al., 2015). Data collection, secondary usage, error, improper access, control and awareness are considered key factors governing control an awareness in the realm of digital privacy (Hong and Thong, 2013). PCT is founded on the principal that the personal data has value, and thus can be exchanged in lieu of currency for services rendered, with each individual forced to consider the benefits and consequences of relinquishing their privacy in each transaction. It has been previously shown that there is positive correlation between a desire for privacy, and perception of risks associated with online services (Baruh et al., 2017; Keith et al., 2013; Liu et al., 2005; Pentina et al., 2016).

3.2.1. Privacy

Digital privacy is a multidimensional (collection, location, accuracy, unauthorised access, unauthorised secondary use) entity that governs the collection and use of personal data (Alraja et al., 2019; Ozturk et al., 2017; Zhang et al., 2013). It has become the primary concern in both IoT and e-commerce due to the sheer volume of inter service data transmission (Baek et al., 2016), with the resultant extreme risk of interception and associated consequences such as forgery and social engineering, identity theft, hacking, unauthorized access, alteration or destruction of information, and eaves dropping (Liaw and Huang, 2013; Osho and Onoja, 2015). The legislative requirements placed upon the healthcare sector provide an additional burden in this regard, in that perceptions of risk associated with HAs are likely to be higher than average due to the need for patient confidentiality. The following hypothesis will explore this in detail:

H3: Privacy has a more significant effect on risk perception toward IoT-enabled HAs among female FHPs than males.

3.2.2. Security

Security is traditionally seen as a means of resource protection, but contemporary definitions must be extended to include software risks such as intrusion, denial of service, forgery, and heterogeneous network attacks (Farash et al., 2016; Jing et al., 2014; Riazul Islam et al., 2015; Sametinger et al., 2015; Weber, 2015). Smith's four dimensional scale (collection, improper access, unauthorised secondary use, error) allows security's effect on BI and risk perception to be considered independently, rather than in tandem with privacy (Bansal and Zahedi, 2014; Gurung and Raja, 2016; Miyazaki and Fernandez, 2000). As the literature has shown that the link between security and e-commerce intentions is stronger in males, the following hypothesis is put forward:

H4: Security has a more significant effect on risk perception toward IoT-enabled HAs among female FHPs than males.

3.3. Trust-risk framework

To predict individuals' intentions towards behaving, adopting, or using any technology, relevant research has indicated that there is ambiguity concerning trust and risk perception's causal relationship. Which is to say, academics have argued about whether trust affects risk perception, or vice versa. Indeed, the following relationships have been found in the reviewed literature: (1) Trust – Risk – Intention (21 studies); (2) Trust – Intention or Risk – Intention (5 studies); (3) Risk – Trust – Intention (6 studies), with more details about these studies being represented in Table (1-b).

A principal reason underpinning this confusion regarding the proposed relationship between trust and risk perception differs according to the type of examined uncertainty (Kim and Koo, 2016). According to Pavlou (2003), this uncertainty may be distinguished into environmental uncertainty (EU) and behavioural uncertainty (BU). The Internet's unpredictable nature is represented by EU. Although providing and ensuring secure transactions is the vendor's responsibility, adopting various tools such as firewalls, authentication, and/or encryption. the online transaction process may still be disturbed via third parties. This refers to how patients' health and personal information may be stolen by hacking attacks, which leads to monetary losses for healthcare institutions (economic risk) in addition to illegal disclosure or misuse of patients' information (privacy risk).

Pavlou (2003) mentioned that web vendors' opportunistic behaviours are associated with behavioural uncertainty, for example the failure to honour warranties, misleading advertising, private information leaks, false identities, as well as product misrepresentation. In the context of IoT-enabled healthcare applications, one must ask whether they are reliable, able to provide good support, as well as enable frontline healthcare providers to care for patients? Healthcare providers may exploit IoT-enabled healthcare services' distant and impersonal characteristics, as well as patients' incapacity to adequately monitor every transaction. This type of uncertainty increases the prospect of unsafe healthcare services (safety risk), in addition to imperfect monitoring by healthcare providers (performance risk) alongside economic and privacy risks.

Despite both environmental and behavioural uncertainty being representative of the risk perception, the majority of the reviewed literature has concentrated on behavioural uncertainty (Kim and Koo, 2016). Dinev and Hart (2006) proposed that trust functions contribute crucially to the diminishing of risk associated with behavioural ambiguity in circumstances where the delivered aid might fail to strongly accord with the personal image or self-conceptualisation of frontline healthcare providers. The delivered aid may fail to fit well with frontline healthcare providers' expectations; healthcare institutions may tolerate the received message, alongside the potential of losing connection during the emergency case, while the devices may fail to transmit the emergency response from the frontline healthcare providers to patients (Dinev and Hart, 2006). Consequently, according to Kim et al.'s (2008) recommendation, formulating trust during the adoption of IoT-based healthcare applications offers a crucial strategy for managing such uncertainty (Kim et al., 2008).

Essentially, the greater trust there is in adopting IoT-based healthcare applications, the lesser the perceptions of risk will be among front healthcare providers. This will subsequently affect their adoption intentions for IoT-based healthcare applications. Furthermore, the majority of the reviewed literature from reputable journals (see Table 1-b) presented the relationship of 'Trust – Risk – Intention', comprising approximately 21 reviewed studies (for example, Arfi et al.'s (2021) study supported this path for IoT in eHealth). On this basis, the current research adopted the trust-risk framework (Mayer et al., 1995a). In this regard, Mayer et al.'s framework is constructed on the assumption that trust governs risk perception, a relationship which is subsequently expressed as attitudes toward a given situation.

Mayer et al.'s framework is built on the assumption that trust governs risk perception, which are then expressed as attitudes toward a given situation. To contextualise this, it is the firm belief that FHPs will both make good use, and take good care of, patient data, that drives users to accept the implementation of IoT-enabled technology.

3.3.1. *Trust*

By definition, trust is a bipartisan approach, whereby one exposes themselves to the other with a strong conviction that their response will be mutually beneficial (Mayer et al., 1995a). Trust has always been critical to evaluating risks, and nowhere is this more apparent than in e-commerce (Gurung and Raja, 2016; Trivedi and Yadav, 2020). Since increasing trust is known to reduce risk, IoT developers must consider how to gain it from users with whom they have no direct interactions if they wish to increase take up and ensure that their product gains widespread acceptance (AlHogail and AlShahrani, 2019; Alraja et al., 2019; Gao and Bai, 2014). As research has shown that women are more conservative in their ability to trust online retailers (Farndale et al., 2011; Kim et al., 2007; McLaughlin et al., 2020), the following hypothesis is proposed:

H5: Trust has a more significant effect on risk perception toward IoT-enabled HAs among female FHPs than males.

3.3.2. *Risk perception*

A major impediment to IoT adoption is that risk perception is a subjective, and hence personal judgement (Alraja et al., 2019; Chaudhuri, 1997; Jalali et al., 2017; Jayashankar et al., 2018). Notwithstanding this, it can be successfully mediated through knowledge transfer from provider to users as a means of increasing comprehension and reducing anxiety in clients (Hsu and Lin, 2018; Li, 2017), which typically reduces negativity towards novel technology (Park et al., 2018). Due to evidence that males are happier to engage in financially risky behaviour (Charness and Gneezy, 2012; Croson and Gneezy, 2009; Garbarino and Strahilevitz, 2004), the following hypotheses are proposed:

H6: Risk perception has a more significant effect on attitude toward Internet of Things (IoT)-enabled healthcare among female FHPs than males.

H7: Risk perception has a more significant effect on BI toward IoT-enabled HAs among female FHPs than males.

4. Methodology

4.1. *Sampling and data collection*

Due to the transient nature of age, it better to categorise by generation than by age group if the wish for ease of generalisation. This implies classification based on year of birth, of which there are four commonly held classes. The oldest, born 1946–1964, are excluded from this study as comparatively few remain within the active workforce. The next two, generations X and Y, form the study population, with the former born 1965-80, and the latter 1981-96. Generation Y are typically considered to be ‘digital natives’ who are technologically reliant and are thus more open to using novel technology such as IoT-enabled HAs (Bolton et al., 2013). The final generation comprises those born 1997–2015, and are not considered herein as the majority are too young to work as FHPs. The end result is a sample that is evenly split between those raised prior to, and those raised with, technology, thus providing ample opportunity to explore gender differences in their BI towards IoT-enabled HAs. In accordance with the research context and the investigated behavioural intention to adopt specific technology (IoT-enabled healthcare applications), this requires respondents to be experts in providing medical treatment to patients in hospitals and medical centres. Consequently, purposive sampling has been adopted as the sampling method, which is reliant upon judgement and intentional identification of typical groups from among the sample (Kerlinger, 1986). This technique permits the inclusion of individuals in the sample based on their specialisation as it relates to the research issue, as well as their ability to provide appropriate data that is relevant and detailed (Jupp, 2006). In this research, the sample was intentionally skewed to include only frontline healthcare services providers (for example doctors), which reflects the research problem (Flyvbjerg, 2006). Furthermore, studies that adopt this technique typically devise specific criteria to determine the respondents’ inclusion, thus ensuring robust external validity and information quality (Apostolopoulos and Liargovas, 2016; Ominde et al., 2021). Therefore, having considered the study purpose, a group of potential respondents were determined in advance based on the following attributes, enabling the selection of targeted respondents. Firstly, respondents should be experts delivering frontline medical treatment, because their knowledge is vital and a prerequisite for responding to the research issue and answering the questionnaire items which are specialised and targeted. Secondly, they should be working in hospitals or medical centres. Thirdly, they should have been born from 1965–80 (generation X), or 1981–96 (generation Y). As a means of collecting the research data, the formulated questionnaire was distributed in hospitals and medical centres across various geographical areas of Oman, thus ensuring a sufficiently representative sample of the target population, which provides a sound justification for the adopted purposive method (Mason, 2002). Regarding sample size, this study adopted the Partial Least Squares (PLS) method, which is a component-based approach and nonparametric technique that does not require normal-distributed input data (Henseler et al., 2009). PLS has been comprehensively approved of and widely adopted among analysts working in the information systems field (Urbach and Ahlemann, 2010), particularly when there is a limited sample size (Goodhue et al., 2006).

In this regard and in accordance with their surveyed literature, Urbach and Ahlemann (2010) determined that the minimum recommended sample size when using PLS ranges between 30 and 100 cases. Furthermore, Apostolopoulos and Liargovas (2016) reviewed the literature regarding purposive sampling, determining that sample size varies according to the research aim. Across all of their reviewed studies, the samples were categorised in different groups, with each group comprising of 2–6 individuals (for more details refer to Apostolopoulos and Liargovas, 2016). Additionally, a purposive sample of 300 respondents was distributed as follows: Male (126); Female (174); age groups 18–30 (118), 31–40 (86), 41–50 (66) and 51+ (30) (Hussain et al., 2017). Another study collected a total of 311 responses using purposive sampling, with the sample distributed as follows: Male (193); Female (118); age groups 18–25 (59), 26–30 (136), as well as 30 and over (120) (Verma et al., 2019). On this basis and as reflected in the reviewed literature, this study’s sample is acceptable for investigating the research hypothesis, given that it comprises of 401 cases distributed as follows: Male (157); Female (244); 117 Gen X and 284 Gen Y individuals. The research model was tested using data collected between April and June of 2020.

4.2. *Measures*

In line with previous publications, the model contained herein adopts the five-point Likert Scale for factor measurement. To measure all the variables in the current study, the constructs were adapted from the existing literature (see Table 2; Appendix (A)).

4.3. *Common method bias (CMB)*

As the data in our study collected from a single respondent, the potential for Common Method Bias (CMB) may be a concern (Podsakoff et al., 2003). To reduce CMB a set of precautions were used both throughout the design and administration of the questionnaire and after the data were gathered.

To judge the validity, reliability and consistency of our first instrument draft, we followed Ping (2004) guidance in our questionnaire design; first a set of experts including (five academicians and five FH experts) were consulted in terms of structure and content. Accordingly, the draft was modified, second a pilot study was conducted using purposive sampling method of 30 FHPs to ensure the validity and reliability

Table 2
Summary of assessed factors.

	Constructs	Number of items	Reference
Security (Sec)	6	(Cheung and Lee, 2000; Connolly and Bannister, 2008; Corbitt et al., 2003; Furnell et al., 2007)	
Privacy (Pri)	3	(Cheung and Lee, 2000; Connolly and Bannister, 2008; Corbitt et al., 2003)	
Trust (Tru)	4	(Gefen et al., 2003; Wu and Chen, 2005)	
Risk Perception (RP)	5	(Cheung and Lee, 2002, 2000)	
Attitude (Att)	4	(Ajzen, 1991; Bhattacherjee, 2000; Galluch and Thatcher, 2011; Gerow et al., 2010; Rana et al., 2019; Taneja et al., 2015; Wu and Chen, 2005)	
Perceived Behavioural Control (PBC)	4	(Bhattacherjee, 2000; Maes et al., 2014; Rana et al., 2019; Taneja et al., 2015; Taylor and Todd, 1995; Wu and Chen, 2005)	
Behavioural Intention (BI)	3	(Galluch and Thatcher, 2011; Gerow et al., 2010; Rana et al., 2019; Taneja et al., 2015; Venkatesh and Davis, 2000, 1996; Wu and Chen, 2005)	

of the questionnaire before disturbing it at big scale (van Teijlingen and Hundley, 2002). The third version then was revised considering the collected feedback resulting a final instrument. All participants as well were briefed on the research aim, with confirmation on the anonymously and confidentiality of their data while encouraging all respondents to answer questions independently and truthfully. Moreover, the adopted constructs were separated randomly in the final distributed questionnaire. After data collection, the Harman's single-factor test was conducted to verify the presence of CMB. The test showed that there were 7 factors with highest variance accounted for the first rotated factor was 30.663% (which is less than 50%) (Podsakoff et al., 2012), indicating that the CMB is not a major concern in our study (Pinzone et al., 2019).

4.4. Analysis process

Once all questionnaires were received we filtered and screened all carefully. The initial phase of screening analysis done using SPSS 23 software. The total number of received cases were 479. However, more investigations of the returned questionnaires resulted in excluding invalid 78 questionnaires as most items were almost the same answers or incomplete replies. Consequently, the valid questionnaires for analysis were 401, which counts for 83.7% of those completed questionnaires in all data collections phases. This number is considered appropriate for analyzing the data using partial least squares (PLS) (Hair et al., 2016). The assessment of the structural model conducted using partial least squares-structural equation modeling (PLS-SEM) using SmartPLS 3.3.2 software. Two main stages were performed to analyse the valid data as: assessing the measurement (validation), and testing the structure model. To test the measurement model, Skewness and Kurtosis statistics test was done to ensure all adopted items were normally distributed. While, the research model reliability was assessed using the Internal consistency reliability (Cronbach's alpha (α) and composite reliability (CR)). Next, the validity of the structure model was assessed using convergent validity (i.e. the average variance extracted AVE), and discriminant validity based on the correlations among latent variables with square root of AVE, cross-loadings, and heterotrait-monotrait ratio (HTMT). Also, a multicollinearity test was conducted prior to the path analysis using the variance inflation factor (VIF) method to check any possible errors arising from the high correlations among the latent variables.

5. Data analysis

Normal distribution of the data was confirmed in SPSS by the kurtosis and skew values (see Table 4), both of which lie between ±2, which represent the limits of normality (Cain et al., 2017). The Partial Least Squares-Structural Equation Model (PLS-SEM) was utilised for the assessment of both the measurement and structural models applied herein (Hair et al., 2019), after which the significance of any difference in gender based path coefficients could be analysed using PLS-Multi Group Analysis (PLS-MGA) (Henseler et al., 2009), with SmartPLS (V.3.3.2) applied to both models using a 5% significance threshold for each group's paths (Henseler et al., 2009).

5.1. Descriptive statistics

The entire sample hold healthcare related basic tertiary qualifications, with 39% holding higher degrees. Sample distributions (see Table 3) are 157:244 for gender (male: female), and 117:284 for generation (X:Y).

5.2. Measurement model

Table 4 provides a summary of the statistics used to determine the reliability, convergent validity, and discriminant validity of the presented model. No factor loading problems were encountered, as is clear from the fact that AVE, Cronbach's alpha, and the composite reliability scores are all above their respective thresholds (0.5, 0.7, and 0.7) (Hair et al., 2014).

Application of the Fornell-Larcker criterion confirmed each construct's discriminant validity, as all showed greater variance within their own indicators than between each other. Meanwhile, cross-loading confirmed that each construct acts primarily on its own indicators. Factors loadings ranked below the 0.5 threshold (Sec4–6, RP4–5) were excluded from further analysis (See appendix A). HTMT analyses (Table 5) showed that the majority of items lay below the threshold (0.85), which allows us to negate the sensitivity shortcomings present in the previous two techniques, and as such to have confidence in the validity of the discriminants used (Henseler et al., 2015).

The level of collinearity (Table 6) was assessed against the Variance Inflation Factor (VIF) threshold (5) (Hair et al., 2014). The results indicate no errors are arising from the high correlations among the latent variables

5.3. Multi-group analysis

It is imperative to confirm the invariance of the model to be applied, since without this it becomes impossible to determine if differences identified are real, or artifices of an inappropriate technique (Sarstedt et al., 2011). Emulating Chin et al.'s approach, item invariance testing was conducted using the MICOM procedure on the gender/generation sample splits (see Table 7). This procedure calls for 2 of 3 conditions to be met—in this case the use of identical PLS models, data treatment and algorithm settings confirmed configural invariance, while the permutation analysis procedure ensured compositional invariance—if a partial measurement invariance condition is to be established for later

Table 3
Demographic profile of study sample.

Gender		Male	Female
		157	244
Age	**Gen X**	56	61
	Gen Y	101	183
Education	**BA Gen X**	27	22
	Postgraduate (or specialist) Gen X	29	39
	BA Gen Y	71	125
	Postgraduate (or specialist) Gen Y	30	58

Table 4
Normality, reliability, and convergent validity.

Constructs	Items	Skewness	Kurtosis	Cronbach's alpha α ≥ 0.70	Loadings	CR ≥ 0.70	AVE ≥0.50
Attitude (Att)	Att 1	-0.253	-0.457	0.798	0.752	0.869	0.624
	Att 2	-0.175	-0.443		0.828		
	Att 3	-0.224	-0.231		0.827		
	Att 4	-0.334	-0.206		0.75		
Behavioural Intention (BI)	BI 1	-0.59	0.111	0.81	0.846	0.886	0.723
	BI 2	-0.737	0.296		0.909		
	BI 3	-0.843	0.349		0.792		
Perceived Behavioural Control (PBC)	PBC 1	-0.144	-0.303	0.78	0.724	0.87	0.692
	PBC 2	-0.229	-0.249		0.848		
	PBC 3	-0.298	-0.345		0.912		
Privacy (Pri)	Pri 1	-0.463	-0.423	0.748	0.81	0.833	0.555
	Pri 2	-0.408	-0.341		0.731		
	Pri 3	-0.428	-0.27		0.708		
	Pri 4	-0.653	0.029		0.727		
Risk Perception (RP)	RP 1	-0.542	0.31	0.797	0.782	0.879	0.708
	RP 2	-0.385	-0.046		0.872		
	RP 3	-0.26	-0.201		0.867		
Security (Sec)	Sec 1	-0.046	-0.76	0.706	0.70	0.832	0.625
	Sec 2	-0.36	-0.243		0.844		
	Sec 3	-0.309	-0.211		0.821		
Trust (Tru)	Tru 1	-0.196	-0.696	0.765	0.726	0.861	0.675
	Tru 2	-0.528	-0.363		0.866		
	Tru 3	-0.574	-0.473		0.865		

Table 5
discriminant validity tests.

Fornell-Larcker criterion							
	Att	BI	PBC	Pri	RP	Sec	Tru
Att	0.79						
BI	0.57	0.85					
PBC	0.64	0.76	0.83				
Pri	0.39	0.36	0.37	0.75			
RP	0.38	0.33	0.31	0.27	0.84		
Sec	0.38	0.31	0.35	0.55	0.33	0.79	
Tru	0.25	0.23	0.20	0.19	0.34	0.18	0.82
HTMT							
	Att	BI	PBC	Pri	RP	Sec	Tru
Att							
BI	0.71						
PBC	0.75	0.84					
Pri	0.49	0.45	0.48				
RP	0.47	0.39	0.37	0.30			
Sec	0.49	0.40	0.45	0.70	0.42		
Tru	0.31	0.26	0.27	0.23	0.42	0.22	

Table 6
VIFs.

Construct	Multicollinearity test		
	Att	BI	RP
Att		1.82	
BI			
PBC		1.72	
Pri			1.45
RP	1	1.18	
Sec			1.44
Tru			1.05

multi-group analysis.

Pairwise assessment of inter and intra generational gender differences was undertaken using Henseler et al.'s nonparametric PLS-MGA technique to distinguish between each groups' path coefficients via a direct comparison of bootstrap estimates for each, assuming a 5% significance threshold in each direction (see Table 8, 9) (Henseler et al., 2009; Sarstedt et al., 2011).

For the moderation role of gender, the results showed all the proposed hypotheses in Gex X not supported as there were no significant differences between the groups (males and females).

For the moderation role of gender in Gex Y, the results showed that H2 (Att-> BI, $P = 0.95$), H5 (Tru -> RP, $P = 0.96$), and H6 (RP -> Att, $P = 0.04$) are supported. All the remained hypotheses were not supported as there were no significant differences between the groups (males and females).

6. Discussion

Aiming to address a distinct gap in the literature, this work assessed gender and generational differences in the factors influencing FHPs BI towards IoT enabled HAs, finding that Gen Y participants exhibited distinct gender based differences in the effect of attitude on BI, risk perception on attitude, and trust on risk perception.

The results in the preceding section allow hypothesis H1 to be rejected, as perceived behavioural control was seen to be significant for all FHPs, regardless of generation or gender—which itself is in direct opposition to previous work (Alzubaidi et al., 2021; Holdsworth et al., 2019; Moon, 2021; Olya et al., 2019). The explanation is offered that the higher than average level of education participants have received, has combined with their extensive decision making experience is likely to improved their ability to assess the usefulness of IoT tools, which in turn is likely to influence their BI.

Acceptance of H2 is dependent on the generation under consideration, with it being supported by Gen Y (in line with previous studies) (Moon, 2021; Olya et al., 2019; Rana et al., 2019; Sommestad et al., 2015), but rejected during analysis of the Gen X cohort. Thus it is suggested that Gen X either holds traditional treatment methods in higher regard, or lacks the confidence to consider implementing new approaches, whereas Gen Y participants are more open to novelty, and consider themselves sufficiently digitally aware to be able to implement it.

The analysis contained herein contradicts work by both Wu et al (2012) and Kim (2015) studies, and rejects the notion set forth in H3 that privacy significantly affects risk perception in a manner that can be differentiated on the basis of gender. This can be explained by considering the differences in privacy and security requirements between medical and commercial settings, and relating this to FHPs' primary concerns being of a technical nature, rather than risk oriented as in the latter. Although H3 is rejected, it is of interest to note that a significant difference in the effect of privacy in risk perception was reported here for Gen X males, who it is suggested are concerned that the increased

Table 7
MICOM Step 2 results for sample groups.

.	Gender Correlation Permutation Mean	5.00%	Permutation p-Values	Age Correlation Permutation Mean	5.00%	Permutation p-Values
Att	0.998	0.995	0.355	0.998	0.995	0.855
BI	0.999	0.998	0.338	0.999	0.998	0.949
PBC	0.999	0.998	0.523	0.999	0.998	0.605
Pri	0.976	0.91	0.12	0.973	0.916	0.473
RP	0.998	0.994	0.926	0.998	0.994	0.219
Sec	0.991	0.973	0.713	0.995	0.981	0.844
Tru	0.994	0.98	0.719	0.993	0.979	0.817

Table 8
Results of PLS-MGA Gen X.

Hypothesis	*P*-Value (Group-diff)	Male Path Coefficients Mean	St.div	*T*-Value	*P*-Value	Female Path Coefficients Mean	St.div	*T*-Value	*P*-Value	Support
Att-> BI	0.65	0.02	0.11	0.07	0.94	0.11	0.16	0.60	0.55	Not supported
PBC-> BI	0.61	0.75	0.08	9.98	0.00	0.67	0.14	4.74	0.00	Not supported
Pri -> RP	0.08	0.32	0.10	2.81	0.01	-0.11	0.29	0.86	0.39	Not supported
RP -> Att	0.72	0.30	0.14	1.92	0.06	0.20	0.15	1.32	0.19	Not supported
RP -> BI	0.46	0.07	0.08	0.98	0.33	0.16	0.13	1.45	0.15	Not supported
Sec-> RP	0.79	0.31	0.12	2.51	0.01	0.27	0.12	2.09	0.04	Not supported
Tru -> RP	0.92	0.26	0.12	2.17	0.03	0.21	0.17	1.30	0.19	Not supported

Table 9
Results of PLS-MGA in Gen Y

Hypothesis	*P*-Value (Group-diff)	Male Path Coefficients Mean	St.div	T-Value	*P*-Value	Female Path Coefficients Mean	St.div	*T*-Value	*P*-Value	Support
Att-> BI	0.95	0.21	0.11	1.98	0.05	0.23	0.07	3.08	0.00	supported
PBC-> BI	0.79	0.64	0.09	7.23	0.00	0.60	0.07	8.68	0.00	Not supported
Pri -> RP	0.13	0.25	0.12	1.99	0.05	0.05	0.08	0.27	0.78	Not supported
RP -> Att	0.04	0.36	0.09	3.94	0.00	0.56	0.06	10.22	0.00	supported
RP -> BI	0.86	0.01	0.07	0.19	0.85	0.03	0.06	0.45	0.66	Not supported
Sec-> RP	0.37	0.18	0.09	1.79	0.07	0.27	0.08	3.28	0.00	Not supported
Tru -> RP	0.96	0.30	0.10	2.90	0.00	0.31	0.06	5.28	0.00	supported

volume of patient data recorded could be associated with them, along with any mistakes made, which in turn could affect their opportunities for advancement.

Consideration of H4 forced its rejection after data analysis, though again it provided results that oppose previous work (McLaughlin et al., 2020), it was found that for Gen X participants, although security was found to significantly affect overall risk perception, there was no discernible difference on the basis of gender. The contrasts slightly with the results for Gen Y, where although the entire cohort were affected by security concerns, H4 was only supported by the fact that females of this generation were more readily influenced than their male counterparts, which goes against McLaughlin et al (2020), who placed the gender divide in the opposite direction. It is suggested that this is the result of women both being more likely to both question judgement calls, and adhere to existing security policies in their personal risk assessment as a result of their chosen career path. In turn, this further highlights the necessity of ensuring awareness of, comprehension of, and compliance with institutional security protocols regardless of gender or generation.

As Gen Y assign significance to trust as a whole, rather than dividing by gender, it is necessary to reject H5 in favour of supporting the existing literature (AlHogail and AlShahrani, 2019). In comparison, the Gen X gender divide first reported by Alraja et al. (2019) is confirmed herein, with only male risk perception significantly affected by trust. The most salient observations herein suggest that while trust remains generally problematic for Gen X, the integration of IoT and healthcare poses a specific barrier to them. The absence of a gender divide suggests that this approach is driven by a desire for traditional interventions, and will require considerable additional training to increase openness in this portion of any given FHP staff. Effectively, this underscores the importance of synthesising trust with the TPB model is intergenerational risk perception is to be properly modelled. This compares well with Gen Y, who are more technologically minded, and hence show greater levels of trust in an HA's ability to support their work. In summary, it is imperative that FHPs have trust, since trust improves risk perception, which in turn improves their behavioural intentions.

The analysis provided in the preceding section shows that, for Gen X at least, H6 must be rejected, since risk perception was found to not significantly affect attitudes toward IoT-enabled HAs. Although previous work has suggested that more perceptive individuals tend to have a correspondingly more positive attitude (Chaudhuri, 1997; Jayashankar et al., 2018), this does not appear to be the case in this instance—perhaps counterintuitively, this is considered to be a by-product of Gen X's aforementioned lack of trust in HAs, which means they fail to give fair assessments of the associated risks as they are written off before this stage. This can be meaningfully compared with Gen Y, who have already been reported as both more trusting, and as having positive BI, and thus it comes as no surprise that, as with previous work (Croson and Gneezy, 2009; Garbarino and Strahilevitz, 2004), while Gen Y's risk perception significantly affects its attitude, this is considerably more apparent in females than in males (Hsu and Lin, 2018).

In contrast with Hsu and Lin (2018), Hypothesis 7 (H7) is also rejected as the data cannot fully support it, instead highlighting the fact that risk perception is insignificant across both generational and gender divides, meaning that there was no discernible difference in BI. It is suggested that this is a result of the ethics within the field of study, where immediate patient care is the primary concern, and thus risks are assessed based on the result of technological failure, rather than a lack of data privacy or security. It appears that while for Gen X, there is no gender divide in their overall perception of risk, they assign different weight to factors—male regard security, privacy and trust equally, whereas females prioritise security. A corresponding assessment of Gen Y shows a clear gender divide, with females rating trust and security as more significant than their male counterparts, who in turn are driven by first trust, and then privacy. This suggests that attitude is perhaps highly influential on the risk perception-behavioural intention relationship.

6.1. Theoretical contributions

Majority of research in IoT field focused on technological aspects. Thus, the foundation for this study lies in that fact that comparatively few studies have considered IoT adoption intention in general, with no previous investigations exploring how this acceptance is mediated by cross-generational female specific attitudes, the intersection of gender difference and multiculturalism, or the gender-generation divide. Moreover, no previous investigations exploring FHPs intention toward IoT-enabled HAs.

There are three key contributions to the literature herein—consideration of gender differences in the behaviour intentions of multicultural FHPs, the design of a novel model to explain these interactions, built from the partial synthesis of TPB, PCT and the trust-risk framework, and finally the application of this model to analyse the effect of generation on novel technology acceptance.

6.2. Practical implications

The presented results show that FHPs in Oman are generally unaware of the risks surrounding IoT-enabled HA implementation, and more pressingly, have little knowledge of their employer's security and privacy protocols. This difficulty is further compounded by the belief that their behaviour is not moderated by their perception of the risks associated with such a take up of new technologies, and thus institutions must ensure that policy is promoted, visible, and comprehensible for both employees and users, with support staff induced to regularly update colleagues on changes to relevant protocols and the consequences of a lack of adherence.

Improved comprehension of privacy, security and trust, and awareness of gender and generational differences is vital for managerial staff wishing to better interpret the BI of their employees. Risk perception in Gen X males is moderated by privacy, trust, and security, whereas female risk perception is governed solely by the latter. This contrasts with Gen Y, wherein privacy and trust are key male predictors, versus trust and security for females, who are also significantly more susceptible to issues surrounding trust than their male counterparts. The upshot of this is that employers must take this into account, and ensure that staff received regular training and access to novel technology if uptake is to be successful

Priority should be given to raising IoT trust in Gen X employers, who are statistically speaking, more suspicious of their usefulness, a fact which has an adverse effect on their overall attitude towards IoT-enabled HAs. As it is attitude, rather than risk perception, which affects BI, behaviour modification training schemes should be used to improve openness to new ideas in their staff. From the perspective of IoT HA development, it is vital that developers liaise with FHPs directly to ensure that the concerns of both parties are adequately addressed before implementation. Institutions are recommended to undergo a period of policy modernisation to ensure that all parties involved with IoT HAs are adequately protected. Key measures of success in this regard are reduced FHP concern and guaranteed patient rights with no reduction in the quality of service provision.

6.3. Limitations and future research directions

The time period in which this study was conducted made it inappropriate to consider Gen Z FHPs, but in the near future this will provide a good topic for further exploration with the aim of direct comparison with the results presented herein. The key conclusion from this work is that trust is paramount, given its effect on risk perception and hence indirectly on attitudes and BI toward IoT-enabled HA implementation in FHPs. The use of a sector specific approach was necessary to provide focus to the study, but it would be of interest to consider other sectors with fewer barriers to entry if more general conclusions are to be drawn.

7. Conclusion

As the majority of the extant literature, has opted to focus on the technological aspects of IoT take up in healthcare, with effectively zero attention paid to the female view, a consideration of the multicultural, bi-generational and gender differences in IoT-enabled HAs' behavioural intentions within FHPs is provided herein, in the hope that it provides support to those in, or managing, the increasing proportion of the workforce who are female.

No differences in BI towards IoT-enabled HAs were observed in Gen X, whereas Gen Y females showed greater levels of significance in the interrelation between BI, attitudes to risk perception and trust. In terms of attitude on BI, risk perception on attitude, and risk perception, no significance was reported for Gen X, whereas the perception of both behavioural control on BI and security on risk showed significance. In this cohort, privacy and trust were shown to only have significance on male BI risk perception. Analysis of the Gen Y cohort showed that attitude on BI, perceived behavioural control on BI, risk perception on attitude, and trust on risk perception all have a significant effect on IoT use, but that risk perception did not significantly affect BI in this group. A distinct gender divide is present in this generation, with males placing greater significance on privacy, whereas females valued security more highly.

Authorship statement

All persons who meet authorship criteria are listed as authors, and all authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted to or published in any other publication before its appearance in the Hong Kong Journal of Occupational Therapy .

Authorship contributions

Contributions made by each author as follows:
Category 1
Conception and design of study: Mansour Alraja;
acquisition of data: Mansour Alraja;
analysis and/or interpretation of data: Mansour Alraja.
Category 2
Drafting the manuscript: Mansour Alraja;
revising the manuscript critically for important intellectual content: Mansour Alraja.
Category 3
Approval of the version of the manuscript to be published:

Declaration of Competing Interest

The author declare that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work is supported by The Research Council (TRC), Sultanate of

Oman (Block Fund-Research Grant), BFP/RGP/ICT/19/186. All persons who have made substantial contributions to the work reported in the manuscript (e.g., technical help, writing and editing assistance, general support), but who do not meet the criteria for authorship, are named in the Acknowledgements and have given us their written permission to be named. If we have not included an Acknowledgements, then that indicates that we have not received substantial contributions from non-authors.

Appendix A: Study measurement

Security	
Sec1	An individual cannot reasonably claim not to have taken an action on-line while they actually have. For example, once an emergency call is placed, the healthcare provider/patient cannot deny placing such a call.
Sec 2	Our hospital/medical centre implement security measures to protect the users.
Sec 3	Our hospital/medical centre usually ensure that treatment information is protected from accidentally altered or destroyed during transmission on the internet.
Sec 4	No one can get access to the data without permission
Sec 5	The used technology in our hospital/medical centre are effective in checking out whether a particular user is authorized to take a certain action
Sec 6	Original content of messages will remain unchanged during or after the on-line treatment.
Privacy	
Pri1	As people should use a true name to receive emergency aid through IoT, hospital/medical centre can ensure the users' personal record will not be misused.
Pri2	Technology mechanism which used in our hospital/medical centre can effectively prevent a third party from stealing on-line people's information.
Pri3	Our hospital/medical centre is concerned about users' privacy.
Pri4	Our hospital/medical centre will not divulge users' personal data to other parties.
Trust	
Tru1	Based on my perception with IoT-enabled healthcare applications, it is reliable
Tru2	Based on my perception with IoT-enabled healthcare applications, it will provide good support.
Tru3	Based on my perception with IoT-enabled healthcare applications, I believe it will help frontline healthcare providers look after patients.
Risk Perception	
RP1	I believe that IoT-enabled healthcare applications are risky because our institution may tolerate the received message.
RP2	I believe that IoT-enabled healthcare applications are risky because of the possibility of losing connection during the emergency case.
RP3	I believe that IoT-enabled healthcare applications are risky because the devices may fail to transmit my emergency response.
RP3	I believe that IoT-enabled healthcare applications are risky because the aid provided may fail to fit well with my personal image or self-concept
RP5	I believe that IoT-enabled healthcare applications are risky because the aid provided may fail to fit well with my expectations.
Attitude	
Att1	I like the idea of using IoT-enabled healthcare applications.
Att2	Using the IoT-enabled healthcare applications for providing healthcare services would be a good idea.
Att3	Using the IoT-enabled healthcare applications for providing healthcare services would be a wise idea.
Att4	Using the IoT-enabled healthcare applications would be a pleasant experience
Perceived Behavioural Control	
PBC1	Using IoT-enabled healthcare applications is entirely up to me.
PBC2	I believe to possess sufficient capacities to use IoT-enabled healthcare applications.
PBC3	I believe I can overcome most obstacles in using IoT-enabled healthcare applications.
Behavioural Intention:	
BI1	Assuming I have access to the IoT-enabled healthcare applications, I intent to use it.
BI2	Given that I have access to the IoT-enabled healthcare applications, I predict that I would use it.
BI3	If I have access to the IoT-enabled healthcare applications, I want to use it as much as possible.

References

Aboobucker, I., Bao, Y., 2018. What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. J. High Technol. Manage. Res. 29, 109–123. https://doi.org/10.1016/j.hitech.2018.04.010.

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Al-Ansi, A., Olya, H.G.T., Han, H., 2019. Effect of general risk on trust, satisfaction, and recommendation intention for halal food. Int. J. Hospital. Manage. 83, 210–219. https://doi.org/10.1016/j.ijhm.2018.10.017.

Al-Debei, M.M., Al-Lozi, E., Papazafeiropoulou, A., 2013. Why people keep coming back to Facebook: Explaining and predicting continuance participation from an extended theory of planned behaviour perspective. Decision Support Syst. 55, 43–54. https://doi.org/10.1016/j.dss.2012.12.032.

Alarabiat, A., Soares, D., Estevez, E., 2021. Determinants of citizens' intention to engage in government-led electronic participation initiatives through Facebook. Govern. Inform. Q. 38, 101537 https://doi.org/10.1016/j.giq.2020.101537.

Albert, L.J., Rodan, S., Aggarwal, N., Hill, T.R., 2019. Gender and generational differences in consumers' perceptions of Internet of Things (IoT) devices. J. Soc. Behav. Res. Bus. 10, 41–53.

Alhasan, A., Audah, L., Ibrahim, I., Al-Sharaa, A., Al-Ogaili, A.S., Mohammed, J, M., 2020. A case-study to examine doctors' intentions to use IoT healthcare devices in Iraq during COVID-19 pandemic. Int. J. Pervasive Comput. Commun. https://doi.org/10.1108/IJPCC-10-2020-0175.

AlHogail, A., AlShahrani, M., 2019. Building Consumer Trust to Improve Internet of Things (IoT) Technology Adoption. Springer, Cham, pp. 325–334. https://doi.org/10.1007/978-3-319-94866-9_33.

Alraja, M.N., Farooque, M.M.J., 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. https://doi.org/10.1109/ACCESS.2019.2904006.

Alzubaidi, H., Slade, E.L., Dwivedi, Y.K., 2021. Examining antecedents of consumers' pro-environmental behaviours: TPB extended with materialism and innovativeness. J. Bus. Res. 122, 685–699. https://doi.org/10.1016/j.jbusres.2020.01.017.

Ameen, N., Tarhini, A., Hussain Shah, M., Madichie, N.O., 2020. Employees' behavioural intention to smartphone security: a gender-based, cross-national study. Comput. Hum. Behav. 104, 106184 https://doi.org/10.1016/j.chb.2019.106184.

Ameen, N., Tarhini, A., Reppel, A., Anand, A., 2021. Customer experiences in the age of artificial intelligence. Comput. Hum. Behav. 114, 106548 https://doi.org/10.1016/j.chb.2020.106548.

Ancker, J.S., Silver, M., Miller, M.C., Kaushal, R., 2013. Consumer experience with and attitudes toward health information technology: a nationwide survey. J. Am. Med. Inform. Assoc. 20, 152–156. https://doi.org/10.1136/amiajnl-2012-001062.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. Comput. Hum. Behav. 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040.

Apostolopoulos, N., Liargovas, P., 2016. Regional parameters and solar energy enterprises: purposive sampling and group AHP approach. Int. J. Energy Sect. Manage. 10, 19–37. https://doi.org/10.1108/IJESM-11-2014-0009.

Arfi, W.Ben, Nasr, I.Ben, 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, 120688. https://doi.org/10.1016/j.techfore.2021.120688.

Asif-Ur-Rahman, M., Afsana, F., Mahmud, M., Shamim Kaiser, M., Ahmed, M.R., Kaiwartya, O., James-Taylor, A., 2019. Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things. IEEE Internet of Things J. 6, 4049–4062. https://doi.org/10.1109/JIOT.2018.2876088.

Azadi, Y., Yazdanpanah, M., Mahmoudi, H., 2019. Understanding smallholder farmers' adaptation behaviors through climate change beliefs, risk perception, trust, and psychological distance: Evidence from wheat growers in Iran. J. Environ. Manage. 250, 109456 https://doi.org/10.1016/j.jenvman.2019.109456.

Baek, S., Seo, S.-H., Kim, S., 2016. Preserving Patient's Anonymity for Mobile Healthcare System in IoT Environment. Int. J. Distrib. Sens. Netw. 12, 2171642 https://doi.org/10.1177/155014772171642.

Bansal, G., Zahedi, F.M., 2014. Trust-discount tradeoff in three contexts: frugality moderating privacy and security concerns. J. Comput. Inform. Syst. 55, 13–29. https://doi.org/10.1080/08874417.2014.11645737.

Bao, F., Chen, I.R., 2012. Trust management for the Internet of Things and its application to service composition, in: 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings. 10.1109/WoWMoM.2012.6263792.

Barnaghi, P., Wang, W., Henson, C., Taylor, K., 2012. Semantics for the internet of things: Early progress and back to the future. Int. J. Semantic Web Inform. Syst. 8, 1–21. https://doi.org/10.4018/jswis.2012010101.

Barth, S., de Jong, M.D.T., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Inform. 34, 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013.

Baruh, L., Secinti, E., Cemalcilar, Z., 2017. Online privacy concerns and privacy management: a meta-analytical review. J. Commun. 67, 26–53. https://doi.org/10.1111/jcom.12276.

Bélanger, F., Carter, L., 2008. Trust and risk in e-government adoption. J. Strat. Inform. Syst. 17, 165–176. https://doi.org/10.1016/j.jsis.2007.12.002.

Ben Arfi, W., Ben Nasr, I., Khvatova, T., Ben Zaied, Y., 2020. Understanding acceptance of eHealthcare by IoT natives and IoT immigrants: an integrated model of UTAUT, perceived risk, and financial cost. Technol. Forecast. Soc. Change 120437. https://doi.org/10.1016/j.techfore.2020.120437.

Bhattacherjee, A., 2000. Acceptance of e-commerce services: the case of electronic brokerages. IEEE Trans. Syst. Man, Cybern. Part A 30, 411–420. https://doi.org/10.1109/3468.852435.

Bolton, R.N., Parasuraman, A., Hoefnagels, A., Migchels, N., Kabadayi, S., Gruber, T., Loureiro, Y.K., Solnet, D., 2013. Understanding generation Y and their use of social media: a review and research agenda. J. Service Manage. 24, 245–267. https://doi.org/10.1108/09564231311326987.

Burda, D., Teuteberg, F., 2014. The role of trust and risk perceptions in cloud archiving - Results from an empirical study. J. High Technol. Manage. Res. 25, 172–187. https://doi.org/10.1016/j.hitech.2014.07.008.

Cai, Z., Fan, X., Du, J., 2017. Gender and attitudes toward technology use: A meta-analysis. Comput. Education 105, 1–13. https://doi.org/10.1016/j.compedu.2016.11.003.

Cain, M.K., Zhang, Z., Yuan, K.-H., 2017. Univariate and multivariate skewness and kurtosis for measuring nonnormality: prevalence, influence and estimation. Behav. Res. Methods 49, 1716–1735. https://doi.org/10.3758/s13428-016-0814-1.

Cassioli, D., Di Marco, A., Di Mascio, T., Tarantino, L., Inverardi, P., 2020. Is really IoT technology gender neutral? 2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2020 - Proceedings. Institute of Electrical and Electronics Engineers Inc., pp. 324–328. https://doi.org/10.1109/MetroInd4.0IoT48571.2020.9138201

Chang, H., Hari, A., Mukherjee, S., Lakshman, T.V., 2014. Bringing the cloud to the edge. IEEE INFOCOM. Institute of Electrical and Electronics Engineers Inc., pp. 346–351. https://doi.org/10.1109/INFCOMW.2014.6849256

Charness, G., Gneezy, U., 2012. Strong evidence for gender differences in risk taking. J. Econ. Behav. Organ. 83, 50–58. https://doi.org/10.1016/j.jebo.2011.06.007.

Chaudhuri, A., 1997. Consumption emotion and perceived risk: a macro-analytic approach. J. Bus. Res. 39, 81–92. https://doi.org/10.1016/S0148-2963(96)00144-0.

Chen, C.C., Hsiao, K.L., Hsieh, C.H., 2019. Understanding usage transfer behavior of two way O2O services. Comput. Hum. Behav. 100, 184–191. https://doi.org/10.1016/j.chb.2018.07.009.

Chen, M., Mao, S., Liu, Y., 2014. Big data: a survey. Mobile Networks Appl. 19, 171–209. https://doi.org/10.1007/s11036-013-0489-0.

Cheung, C., Lee, M., 2002. Trust in internet shopping:instrument development and validation through classical and modern approaches. In: Fazlollahi, B. (Ed.), Strategies for ECommerce Success. IGI Global, pp. 126–145. https://doi.org/10.4018/978-1-931777-08-7.ch008.

Cheung, C., Lee, M., 2000. Trust in internet shopping: a proposed model and measurement instrument. AMCIS 2000 Proceedings.

Chin, A.G., Harris, M.A., Brookshire, R., 2018. A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. Int. J. Inf. Manage. 39, 49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010.

Compeau, D.R., Higgins, C.A., 1995. Computer self-efficacy: development of a measure and initial test. MIS Q. 19, 189–210. https://doi.org/10.2307/249688.

Connolly, R., Bannister, F., 2008. Factors influencing Irish consumers' trust in internet shopping. Manage. Res. News 31, 339–358. https://doi.org/10.1108/01409170810865154.

Corbitt, B.J., Thanasankit, T., Yi, H., 2003. Trust and e-commerce: a study of consumer perceptions. Electron. Commerce Res. Appl. 2, 203–215. https://doi.org/10.1016/S1567-4223(03)00024-3.

Croson, R., Gneezy, U., 2009. Gender differences in preferences. J. Econ. Lit. 47, 448–474. https://doi.org/10.1257/jel.47.2.448.

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organ. Sci. 10, 104–115. https://doi.org/10.1287/orsc.10.1.104.

Dinev, T., Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. 17, 61–80. https://doi.org/10.1287/isre.1060.0080.

Farash, M.S., Turkanović, M., Kumari, S., Hölbl, M., 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks 36, 152–176. https://doi.org/10.1016/J.ADHOC.2015.05.014.

Farndale, E., Van Ruiten, J., Kelliher, C., Hope-Hailey, V., 2011. The influence of perceived employee voice on organizational commitment: An exchange perspective. Hum. Resour. Manage. 50, 113–129. https://doi.org/10.1002/hrm.20404.

Flyvbjerg, B., 2006. Five misunderstandings about case-study research. Qual. Inquiry 12, 219–245. https://doi.org/10.1177/1077800405284363.

Fosso Wamba, S., Akter, S., Edwards, A., Chopin, G., Gnanzou, D., 2015. How "big data" can make big impact: findings from a systematic review and a longitudinal case study. Int. J. Prod. Econ. 165, 234–246. https://doi.org/10.1016/j.ijpe.2014.12.031.

Furnell, S.M., Bryant, P., Phippen, A.D., 2007. Assessing the security perceptions of personal Internet users. Comput. Security 26, 410–417. https://doi.org/10.1016/J.COSE.2007.03.001.

Galluch, P., Thatcher, J., 2011. Maladaptive vs. faithful use of internet applications in the classroom: an empirical examination. J. Inform. Technol. Theory Appl. (JITTA) 12.

Gao, L., Bai, X., 2014. A unified perspective on the factors influencing consumer acceptance of internet of things technology. Asia Pacific J. Market. Logistics 26, 211–231. https://doi.org/10.1108/APJML-06-2013-0061.

Garbarino, E., Strahilevitz, M., 2004. Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. J. Bus. Res. 57, 768–775. https://doi.org/10.1016/S0148-2963(02)00363-6.

Gefen, D., Karahanna, E., Straub, D.W., 2003. Trust and TAM in online shopping: AN integrated model. MIS Q. 27, 51–90. https://doi.org/10.2307/30036519.

Gerow, J., Galluch, P.S., Thatcher, J., 2010. To slack or not to slack: internet usage in the classroom. The J. Inform. Technol. Theory Appl. 11.

Goodhue, D., Lewis, W., Thompson, R., 2006. PLS, small sample size, and statistical power in MIS research, in: Proceedings of the Annual Hawaii International Conference on System Sciences. 10.1109/HICSS.2006.381.

Gurung, A., Raja, M.K., 2016. Online privacy and security concerns of consumers. Inform. Comput. Security 24, 348–371. https://doi.org/10.1108/ICS-05-2015-0020.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2016. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed. Sage Publishing. https://doi.org/10.1007/s10995-012-1023-x [doi].

Hair, J.F., Sarstedt, M., Hopkins, L., Kuppelwieser, V.G., 2014. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. Eur. Bus. Rev.. 10.1108/EBR-10-2013-0128.

Hair, J.F., Sarstedt, M., Ringle, C.M., 2019. Rethinking some of the rethinking of partial least squares. Eur. J. Market. 53, 566–584. https://doi.org/10.1108/EJM-10-2018-0665.

Hakim, M.P., Zanetta, L.D.A., de Oliveira, J.M., da Cunha, D.T., 2020. The mandatory labeling of genetically modified foods in Brazil: consumer's knowledge, trust, and risk perception. Food Res. Int. 132, 109053 https://doi.org/10.1016/j.foodres.2020.109053.

Hann, I.H., Hui, K.L., Lee, S.Y.T., Png, I.P.L., 2007. Overcoming online information privacy concerns: an information-processing theory approach. J. Manage. Inform. Syst. 24, 13–42. https://doi.org/10.2753/MIS0742-1222240202.

Hansen, J.M., Saridakis, G., Benson, V., 2018. Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. Comput. Hum. Behav. 80, 197–206. https://doi.org/10.1016/j.chb.2017.11.010.

Hasan, R., Shams, R., Rahman, M., 2020. Consumer trust and perceived risk for voice-controlled artificial intelligence: the case of Siri. J. Bus. Res.. 10.1016/j.jbusres.2020.12.012.

Hassan, N., Gillani, S., Ahmed, E., Yaqoob, I., Imran, M., 2018. The role of edge computing in Internet of Things. IEEE Commun. Mag. 56, 110–115. https://doi.org/10.1109/MCOM.2018.1700906.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Market. Sci. 43, 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Henseler, J., Ringle, C.M., Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing. Adv. Int. Market. 20, 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014.

Holdsworth, S., Sandri, O., Thomas, I., Wong, P., Chester, A., McLaughlin, P., 2019. The assessment of graduate sustainability attributes in the workplace: potential advantages of using the theory of planned behaviour (TPB). J. Cleaner Prod. 238, 117929 https://doi.org/10.1016/j.jclepro.2019.117929.

Hong, W., Thong, J.Y.L., 2013. Internet privacy concerns: an integrated conceptualization and four empirical studies. MIS Q. 37, 275–298. https://doi.org/10.25300/MISQ/2013/37.1.12.

Hou, J., Elliott, K., 2016. Gender differences in online auctions. Electron. Commerce Res. Appl. 17, 123–133. https://doi.org/10.1016/j.elerap.2016.04.004.

Hsu, C.-L., Lin, J.C.-C., 2018. Exploring factors affecting the adoption of internet of things services. J. Comput. Inform. Syst. 58, 49–57. https://doi.org/10.1080/08874417.2016.1186524.

Hussain, S., Ahmed, W., Jafar, R.M.S., Rabnawaz, A., Jianzhou, Y., 2017. eWOM source credibility, perceived risk and food product customer's information adoption. Comput. Hum. Behav. 66, 96–102. https://doi.org/10.1016/j.chb.2016.09.034.

Ifinedo, P., 2014. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inform. Manage. 51, 69–79. https://doi.org/10.1016/j.im.2013.10.001.

Jalali, M.S., Kaiser, J.P., Siegel, M., Madnick, S., 2017. The Internet of Things (IoT) Promises New Benefits And Risks: A Systematic Analysis of Adoption Dynamics of IoT Products. SSRN Electronic Journal. 10.2139/ssrn.3022111.

Jayashankar, P., Nilakanta, S., Johnston, W.J., Gill, P., Burres, R., 2018. IoT adoption in agriculture: the role of trust, perceived value and risk. J. Bus. Indus. Market. 33, 804–821. https://doi.org/10.1108/JBIM-01-2018-0023.

Jin, J., Gubbi, J., Marusic, S., Palaniswami, M., 2014. An information framework for creating a smart city through internet of things. IEEE Internet of Things J. 1, 112–121. https://doi.org/10.1109/JIOT.2013.2296516.

Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D., 2014. Security of the Internet of Things: perspectives and challenges. Wireless Networks 20, 2481–2501. https://doi.org/10.1007/s11276-014-0761-7.

Jozani, M., Ayaburi, E., Ko, M., Choo, K.K.R., 2020. Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective. Comput. Hum. Behav. 107, 106260 https://doi.org/10.1016/j.chb.2020.106260.

Jupp, V., 2006. The SAGE Dictionary of Social Research Methods.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. Int. J. Hum. Comput. Studies 71, 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016.

Kerlinger, F.N., 1986. Foundations of Behavioral Research, 3rd ed, American Educational Research Journal. Wadsworth Publishing.

Khalilzadeh, J., Ozturk, A.B., Bilgihan, A., 2017. Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. Comput. Hum. Behav. 70, 460–474. https://doi.org/10.1016/j.chb.2017.01.001.

Kim, D.J., Ferrin, D.L., Rao, H.R., 2008. A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decision Support Syst. 44, 544–564. https://doi.org/10.1016/j.dss.2007.07.001.

Kim, D.Y., Lehto, X.Y., Morrison, A.M., 2007. Gender differences in online travel information search: implications for marketing communications on the internet. Tourism Manage. 28, 423–433. https://doi.org/10.1016/j.tourman.2006.04.001.

Kim, G., Koo, H., 2016. The causal relationship between risk and trust in the online marketplace: a bidirectional perspective. Comput. Hum. Behav. 55, 1020–1029. https://doi.org/10.1016/j.chb.2015.11.005.

Knauder, H., Koschmieder, C., 2019. Individualized student support in primary school teaching: a review of influencing factors using the theory of planned behavior (TPB). Teaching Teacher Education 77, 66–76. https://doi.org/10.1016/j.tate.2018.09.012.

Lai, M., Lin, S.-M., Wu, W.-Y., 2008. A qualitative approach for conceptualizing consumer decision-making in online auctions. In: Lee, A.Y., Soman, D. (Eds.), Advances in Consumer Research. Association for Consumer Research, pp. 319–324.

Li, H., Sarathy, R., Xu, H., 2011. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Syst. 51, 434–445. https://doi.org/10.1016/j.dss.2011.01.017.

Li, L., 2017. An investigation on the Risk Perception of Residents in IoT Smart Home Environments. Eindhoven University of Technology.

Li, X., Dai, H.N., Wang, Q., Imran, M., Li, D., Imran, M.A., 2020. Securing Internet of Medical Things with Friendly-jamming schemes. Computer Communications. 10.1016/j.comcom.2020.06.026.

Liao, C., Chen, J.L., Yen, D.C., 2007. Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: an integrated model. Comput. Hum. Behav. 23, 2804–2822. https://doi.org/10.1016/j.chb.2006.05.006.

Liaw, S.S., Huang, H.M., 2013. Perceived satisfaction, perceived usefulness and interactive learning environments as predictors to self-regulation in e-learning environments. Comput. Educ. 60, 14–24. https://doi.org/10.1016/j.compedu.2012.07.015.

Liébana-Cabanillas, F., Molinillo, S., Ruiz-Montañez, M., 2019. To use or not to use, that is the question: analysis of the determining factors for using NFC mobile payment systems in public transportation. Technol. Forecast. Social Change 139, 266–276. https://doi.org/10.1016/j.techfore.2018.11.012.

Liu, C., Marchewka, J.T., Lu, J., Yu, C.S., 2005. Beyond concern-a privacy-trust-behavioral intention model of electronic commerce. Inform. Manage. 42, 289–304. https://doi.org/10.1016/j.im.2004.01.003.

Luo, X., Li, H., Zhang, J., Shim, J.P., 2010. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. Decision Support Syst. 49, 222–234. https://doi.org/10.1016/j.dss.2010.02.008.

Lv, Z., Song, H., Basanta-Val, P., Steed, A., Jo, M., 2017. Next-generation big data analytics: state of the art, challenges, and future research topics. IEEE Trans. Ind. Inf. 13, 1891–1899. https://doi.org/10.1109/TII.2017.2650204.

Madichie, N.O., Gallant, M., 2012. Broken silence: a commentary on women's entrepreneurship in the United Arab Emirates. The Int. J. Entrepreneur. Innov. 13, 81–92. https://doi.org/10.5367/ijei.2012.0071.

Maes, J., Leroy, H., Sels, L., 2014. Gender differences in entrepreneurial intentions: a TPB multi-group analysis at factor and indicator level. Eur. Manage. J. 32, 784–794. https://doi.org/10.1016/j.emj.2014.01.001.

Mamonov, S., Benbunan-Fich, R., 2018. The impact of information security threat awareness on privacy-protective behaviors. Comput. Hum. Behav. 83, 32–44. https://doi.org/10.1016/j.chb.2018.01.028.

Marett, K., Pearson, A.W., Pearson, R.A., Bergiel, E., 2015. Using mobile devices in a high risk context: the role of risk and trust in an exploratory study in Afghanistan. Technol. Soc. 41, 54–64. https://doi.org/10.1016/j.techsoc.2014.11.002.

Mariani, M.M., Ek Styven, M., Teulon, F., 2021. Explaining the intention to use digital personal data stores: an empirical study. Technol. Forecast. Soc. Change 166, 120657. https://doi.org/10.1016/j.techfore.2021.120657.

Marriott, H.R., Williams, M.D., 2018. Exploring consumers perceived risk and trust for mobile shopping: a theoretical framework and empirical study. J. Retail. Consumer Services 42, 133–146. https://doi.org/10.1016/j.jretconser.2018.01.017.

Mason, J., 2002. Qualitative Researching, 2nd ed. SAGE Publications Ltd, London, UK.

Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995a. An integrative model of organizational trust. Acad. Manage. Rev. 20, 709. https://doi.org/10.2307/258792.

Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995b. An integrative model of organizational trust. Acad. Manage. Rev. 20, 734. https://doi.org/10.2307/258792.

McLaughlin, C., McCauley, L.B., Prentice, G., Verner, E.J., Loane, S., 2020. Gender differences using online auctions within a generation Y sample: an application of the theory of planned behaviour. J. Retail. Consumer Services 56, 102181. https://doi.org/10.1016/j.jretconser.2020.102181.

Miltgen, C.L., Smith, H.J., 2015. Exploring information privacy regulation, risks, trust, and behavior. Inform. Manage. 52, 741–759. https://doi.org/10.1016/j.im.2015.06.006.

Miyazaki, A.D., Fernandez, A., 2000. Internet privacy and security: an examination of online retailer disclosures. J.Public Policy & Market. 19, 54–61. https://doi.org/10.1509/jppm.19.1.54.16942.

Montano, D., Kasprzyk, D., 2015. Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In: Glanz, K., Rimer, B.K., Viswanath, K. (Eds.), Health Behavior: Theory, Research, and Practice. Jossey-Bass.

Moon, S.J., 2021. Investigating beliefs, attitudes, and intentions regarding green restaurant patronage: An application of the extended theory of planned behavior with moderating effects of gender and age. Int. J. Hospital. Manage. 92, 102727 https://doi.org/10.1016/j.ijhm.2020.102727.

Morris, M.G., Venkatesh, V., Ackerman, P.L., 2005. Gender and age differences in employee decisions about new technology: an extension to the theory of planned behavior. IEEE Trans. Eng. Manage. 52, 69–84. https://doi.org/10.1109/TEM.2004.839967.

Mueller, C.E., 2020. Examining the inter-relationships between procedural fairness, trust in actors, risk expectations, perceived benefits, and attitudes towards power grid expansion projects. Energy Policy 141, 111465. https://doi.org/10.1016/j.enpol.2020.111465.

Nami, F., Vaezi, S., 2018. How ready are our students for technology-enhanced learning? Students at a university of technology respond. J. Comput. Higher Education 30, 510–529. https://doi.org/10.1007/s12528-018-9181-5.

NCSI, 2020. National Centre for Statistics and information (NCSI). NCSI Portal. [WWW Document]URL https://www.ncsi.gov.om/Pages/NCSI.aspx (accessed 12.1.20).

Nicolaou, A.I., Ibrahim, M., Van Heck, E., 2013. Information quality, trust, and risk perceptions in electronic data exchanges. Decision Support Syst. 54, 986–996. https://doi.org/10.1016/j.dss.2012.10.024.

Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G., 2012. A subjective model for trustworthiness evaluation in the social Internet of Things. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC, pp. 18–23. https://doi.org/10.1109/PIMRC.2012.6362662.

Olya, H.G.T., Bagheri, P., Tümer, M., 2019. Decoding behavioural responses of green hotel guests: a deeper insight into the application of the theory of planned behaviour. Int. J. Contemporary Hospital. Manage. 31, 2509–2525. https://doi.org/10.1108/IJCHM-05-2018-0374.

Ominde, D., Godfrey Ochieng, E., Oteke Omwenga, V., 2021. Optimising ICT infrastructure performance in developing countries: Kenyan viewpoint. Technol. Forecast. Social Change 169, 1–14. https://doi.org/10.1016/j.techfore.2021.120844.

Ortega Egea, J.M., Román González, M.V., 2011. Explaining physicians' acceptance of EHCR systems: An extension of TAM with trust and risk factors. Comput. Hum. Behav. 27, 319–332. https://doi.org/10.1016/j.chb.2010.08.010.

Osho, O., Onoja, A.D., 2015. National cyber security policy and strategy of Nigeria: a qualitative analysis. Int. J. Cyber Criminol. 9, 120–143. https://doi.org/10.5281/zenodo.22390.

Ozturk, A.B., Nusair, K., Okumus, F., Singh, D., 2017. Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. Inform. Syst. Front. 19, 753–767. https://doi.org/10.1007/s10796-017-9736-4.

Pang, Z., Chen, Q., Han, W., Zheng, L., 2015. Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion. Inform. Syst. Front. 17, 289–319. https://doi.org/10.1007/s10796-012-9374-9.

Park, C., Kim, Y., Jeong, M., 2018. Influencing factors on risk perception of IoT-based home energy management services. Telematics Inform. 35, 2355–2365. https://doi.org/10.1016/j.tele.2018.10.005.

Pavlou, P.A., 2003. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. Int. J. Electron. Commerce 7, 101–134. https://doi.org/10.2307/27751067.

Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Comput. Hum. Behav. 65, 409–419. https://doi.org/10.1016/j.chb.2016.09.005.

Perera, G., Holbrook, A., Thabane, L., Foster, G., Willison, D.J., 2011. Views on health information sharing and privacy from primary care practices using electronic medical records. Int. J. Med. Inf. 80, 94–101. https://doi.org/10.1016/j.ijmedinf.2010.11.005.

Pillai, R., Sivathanu, B., 2020. Adoption of internet of things (IoT) in the agriculture industry deploying the BRT framework. Benchmarking 27, 1341–1368. https://doi.org/10.1108/BIJ-08-2019-0361.

Ping, R.A., 2004. On assuring valid measures for theoretical models using survey data. J. Bus. Res. 57, 125–141. https://doi.org/10.1016/S0148-2963(01)00297-1.

Pinzone, M., Guerci, M., Lettieri, E., Huisingh, D., 2019. Effects of 'green' training on pro-environmental behaviors and job satisfaction: Evidence from the Italian healthcare sector. J. Cleaner Prod. 226, 221–232. https://doi.org/10.1016/j.jclepro.2019.04.048.

Plaza, I., Martín, L., Martin, S., Medrano, C., 2011. Mobile applications in an aging society: status and trends. J. Syst. Software 84, 1977–1988. https://doi.org/10.1016/j.jss.2011.05.035.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88, 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of method bias in social science research and recommendations on how to control it. Annu. Rev. Psychol. 63, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452.

Priyadarshinee, P., Raut, R.D., Jha, M.K., Gardas, B.B., 2017. Understanding and predicting the determinants of cloud computing adoption: a two staged hybrid SEM - neural networks approach. Comput. Hum. Behav. 76, 341–362. https://doi.org/10.1016/j.chb.2017.07.027.

Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R.U., Dou, W., 2020. Complementing IoT services through software defined networking and edge computing: a comprehensive survey. IEEE Commun. Surveys Tutorials 22, 1761–1804. https://doi.org/10.1109/COMST.2020.2997475.

Rana, N.P., Slade, E., Kitching, S., Dwivedi, Y.K., 2019. The IT way of loafing in class: Extending the theory of planned behavior (TPB) to understand students' cyberslacking intentions. Comput. Hum. Behav. 101, 114–123. https://doi.org/10.1016/j.chb.2019.07.022.

Raut, R.D., Priyadarshinee, P., Gardas, B.B., Jha, M.K., 2018. Analyzing the factors influencing cloud computing adoption using three stage hybrid SEM-ANN-ISM (SEANIS) approach. Technol. Forecast. Social Change 134, 98–123. https://doi.org/10.1016/j.techfore.2018.05.020.

Raza, S.A., Qazi, W., Shah, N., Qureshi, M.A., Qaiser, S., Ali, R., 2020. Drivers of intensive Facebook usage among university students: An implications of U&G and TPB theories. Technol. Soc. 62, 101331 https://doi.org/10.1016/j.techsoc.2020.101331.

Razzak, M.I., Imran, M., Xu, G., 2020. Big data analytics for preventive medicine. Neural Comput. Appl. 32, 4417–4451. https://doi.org/10.1007/s00521-019-04095-y.

Riazul Islam, S.M., Daehan, Kwak, Humaun Kabir, M., Hossain, M., Kyung-Sup, Kwak, 2015. The internet of things for health care: a comprehensive survey. IEEE Access 3, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951.

Riedl, R., Hubert, M., Kenning, P., 2010. Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers. MIS Q. 34, 397–428. https://doi.org/10.2307/20721434.

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I.M., Montero, R., Wolfsthal, Y., Elmroth, E., Cáceres, J., Ben-Yehuda, M., Emmerich, W., Galán, F., 2009. The Reservoir model and architecture for open federated cloud computing. IBM J. Res. Dev. 53 https://doi.org/10.1147/JRD.2009.5429058.

Rouibah, K., Lowry, P.B., Hwang, Y., 2016. The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. Electron. Commerce Res. Appl. 19, 33–43. https://doi.org/10.1016/j.elerap.2016.07.001.

Rubinstein, I., 2013. Big data: the end of privacy or a new beginning? Int. Data Privacy Law 3, 74–87. https://doi.org/10.2139/ssrn.2157659.

Sametinger, J., Rozenblit, J., Lysecky, R., Ott, P., 2015. Security challenges for medical devices. Commun. ACM 58, 74–82. https://doi.org/10.1145/2667218.

Sarstedt, M., Henseler, J., Ringle, C.M., 2011. Multigroup analysis in partial least squares (PLS) path modeling: alternative methods and empirical results. Adv. Int. Market. 22, 195–218. https://doi.org/10.1108/S1474-7979(2011)0000022012.

Shah, M.H., Peikari, H.R., Yasin, N.M., 2014. The determinants of individuals' perceived e-security: evidence from Malaysia. Int. J. Inf. Manage. 34, 48–57. https://doi.org/10.1016/j.ijinfomgt.2013.10.001.

Shiau, W.L., Chau, P.Y.K., 2016. Understanding behavioral intention to use a cloud computing classroom: a multiple model comparison approach. Inform. Manage. 53, 355–365. https://doi.org/10.1016/j.im.2015.10.004.

Sommestad, T., Karlzén, H., Hallberg, J., 2015. The sufficiency of the theory of planned behavior for explaining information security policy compliance. Inform. Comput. Security 23, 200–217. https://doi.org/10.1108/ICS-04-2014-0025.

Sun, Y., Song, H., Jara, A.J., Bie, R., 2016. Internet of things and big data analytics for smart and connected communities. IEEE Access 4, 766–773. https://doi.org/10.1109/ACCESS.2016.2529723.

Sun, Y., Wang, N., Shen, X.L., Zhang, J.X., 2015. Location information disclosure in location-based social network services: privacy calculus, benefit structure, and gender differences. Comput. Hum. Behav. 52, 278–292. https://doi.org/10.1016/j.chb.2015.06.006.

Syed, L., Jabeen, S., S, M., Alsaeedi, A., 2019. Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques. Future Gener. Comput. Syst. 101, 136–151. https://doi.org/10.1016/j.future.2019.06.004.

Taneja, A., Fiore, V., Fischer, B., 2015. Cyber-slacking in the classroom: potential for digital distraction in the new age. Comput. Educ. 82, 141–151. https://doi.org/10.1016/j.compedu.2014.11.009.

Tarhini, A., Deh, R.M., Al-Busaidi, K.A., Mohammed, A.B., Maqableh, M., 2017. Factors influencing students' adoption of e-learning: a structural equation modeling approach. J. Int. Educ. Business 10, 164–182. https://doi.org/10.1108/JIEB-09-2016-0032.

Taylor, S., Todd, P.A., 1995. Understanding Information Technology Usage: A Test of Competing Models. Inf. Syst. Res. 6, 144–176.

Tewari, A., Gupta, B.B., 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Gener. Comput. Syst. 108, 909–920. https://doi.org/10.1016/j.future.2018.04.027.

Thusi, P., Maduku, D.K., 2020. South African millennials' acceptance and use of retail mobile banking apps: an integrated perspective. Comput. Hum. Behav. 111, 106405 https://doi.org/10.1016/j.chb.2020.106405.

Trivedi, S.K., Yadav, M., 2020. Repurchase intentions in Y generation: mediation of trust and e-satisfaction. Market. Intell. Plann. 38, 401–415. https://doi.org/10.1108/MIP-02-2019-0072.

Tu, M., 2018. An exploratory study of internet of things (IoT) adoption intention in logistics and supply chain management a mixed research approach. International Journal of Logistics Management. Emerald Group Publishing Ltd., pp. 131–151. https://doi.org/10.1108/IJLM-11-2016-0274

Urbach, N., Ahlemann, F., 2010. Structural equation modeling in information systems research using partial least squares. J. Inform. Technol. Theory Appl. (JITTA) 11.

van Riper, C.J., Wallen, K.E., Landon, A.C., Petriello, M.A., Kyle, G.T., Absher, J., 2016. Modeling the trust-risk relationship in a wildland recreation setting: a social exchange perspective. J. Outdoor Recreat. Tourism 13, 23–33. https://doi.org/10.1016/j.jort.2016.03.001.

van Teijlingen, E., Hundley, V., 2002. The importance of pilot studies. Nursing standard. Royal College of Nursing (Great Britain), p. 1987. https://doi.org/10.7748/ns2002.06.16.40.33.c3214. :

Venkatesh, V., Davis, F.D., 2000. Theoretical extension of the technology acceptance model: four longitudinal field studies. Manage. Sci. 46, 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926.

Venkatesh, V., Davis, F.D., 1996. A model of the antecedents of perceived ease of use: development and test. Decision Sci. 27, 451–481. https://doi.org/10.1111/j.1540-5915.1996.tb00860.x.

Verma, V.K., Chandra, B., Kumar, S., 2019. Values and ascribed responsibility to predict consumers' attitude and concern towards green hotel visit intention. J. Bus. Res. 96, 206–216. https://doi.org/10.1016/j.jbusres.2018.11.021.

Wang, C., Bi, Z., Xu, L.Da, 2014. IoT and cloud computing in automation of assembly modeling systems. IEEE Trans. Ind. Inf. 10, 1426–1434. https://doi.org/10.1109/TII.2014.2300346.

Wang, Y., Min, Q., Han, S., 2016. Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. Comput. Hum. Behav. https://doi.org/10.1016/j.chb.2015.11.011.

Weber, R.H., 2015. Internet of things: privacy issues revisited. Comput. Law & Secur. Rev. 31, 618–627. https://doi.org/10.1016/J.CLSR.2015.07.002.

Win, K.T., 2005. A review of security of electronic health records. Health Inf. Manag. 34, 13–18. https://doi.org/10.1177/183335830503400105.

World Economic Forum, 2020. Global Gender Gap Report.

Wu, D., Lowry, P.B., Zhang, D., Parks, R.F., 2021. Patients' compliance behavior in a personalized mobile patient education system (PMPES) setting: rational, social, or personal choices? Int. J. Med. Inf. 145, 104295 https://doi.org/10.1016/j.ijmedinf.2020.104295.

Wu, I.L., Chen, J.L., 2005. An extension of trust and TAM model with TPB in the initial adoption of on-line tax: an empirical study. Int. J. Human Comput. Studies 62, 784–808. https://doi.org/10.1016/j.ijhcs.2005.03.003.

Yan, Z., Zhang, P., Vasilakos, A.V., 2014. A survey on trust management for Internet of Things. J. Netw. Comput. Appl. 42, 120–134. https://doi.org/10.1016/j.jnca.2014.01.014.

Yang, H., Lee, W., Lee, H., 2018. IoT smart home adoption: the importance of proper level automation. J. Sensors 2018, 1–11. https://doi.org/10.1155/2018/6464036.

Yang, Q., Pang, C., Liu, L., Yen, D.C., Michael Tarn, J., 2015. Exploring consumer perceived risk and trust for online payments: an empirical study in China's younger generation. Comput. Hum. Behav. 50, 9–24. https://doi.org/10.1016/j.chb.2015.03.058.

Yao, X., Farha, F., Li, R., Psychoula, I., Chen, L., Ning, H., 2020. Security and privacy issues of physical objects in the IoT: Challenges and opportunities. Digital Communications and Networks. 10.1016/j.dcan.2020.09.001.

Ye, M., Lyu, Z., 2020. Trust, risk perception, and COVID-19 infections: evidence from multilevel analyses of combined original dataset in China. Soc. Sci. Med. 265, 113517 https://doi.org/10.1016/j.socscimed.2020.113517.

Yildirim, H., Ali-Eldin, A.M.T., 2019. A model for predicting user intention to use wearable IoT devices at the workplace. J. King Saud University - Comput. Inform. Sci. 31, 497–505. https://doi.org/10.1016/j.jksuci.2018.03.001.

Zhang, R., Chen, J.Q., Jaejung Lee, C.A., 2013. Mobile commerce and consumer privacy concerns. J. Comput. Inform. Syst. 53, 31–38. https://doi.org/10.1080/08874417.2013.11645648.

Mansour Naser Alraja received the PhD degree in management information systems (2010). He is currently an associate professor of management information systems (MIS) with the Department of MIS, College of Commerce and Business Administration, Dhofar University, Oman. His research interests include information technology adoption, data analytics, information security, e-commerce, and the IoT. Alraja published many papers in many reputable journals that are indexed in Web of Science and have an impact factor. He has also served as a reviewer for many well-reputed conferences, including AOM, AIB, and IEEE conferences, as well as acting as a reviewer for several reputable journals such the Journal of Small Business & Entrepreneurship, IEEE Access, and Sage open. Alraja is College's Chief Accreditation Officer for AACSB. Moreover, since 2018, he has been appointed as the Chair for the Department of MIS. Alraja was a principle investigator for many funded projects. Currently, he is leading and mentoring two funded research project. Moreover, out of his research work he has many accepted and under review papers in very good journals (ABS 4, ABS 3 and ABS 2). Currently, he is guest editor in the International Journal of Emergency Services (ABS 2).