IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 31, 2019, accepted February 21, 2019, date of publication March 8, 2019, date of current version August 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2904006

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

MANSOUR NASER ALRAJA[1], MURTAZA MOHIUDDIN JUNAID FAROOQUE[1], AND BASEL KHASHAB[2]

[1]Department of Management Information Systems, Dhofar University, Salalah 2509, Oman
[2]Northumbria University—London Campus, London E1 7HT, U.K.

Corresponding author: Mansour Naser Alraja (malraja@du.edu.om)

ABSTRACT The Internet of Things (IoT) refers to the network of devices which contain electronics, sensors or software that enables them to connect at anytimeand anywhere through a cyber-physical system. Before the establishment of such a system, it should be considered to what extent the users are ready to adopt and use it in their daily routines. Therefore, this paper explores users' attitudestowardsusing IoT technologies to receive healthcare services. This is in contrast to most previous research, which has studied the technical requirements or devices of the IoT that are required in healthcare services, or ways in which connectivity and performance can be improved using the IoT. Based on known models of technology acceptance, an integrated framework was developed to investigate the impact of security and privacy concerns, and familiarity with the technology, on users' trust in the IoT, and then to measure the effect of that trust on Omani users' attitudes regarding use ofIoT technologies to receive healthcare services. This framework enabled the measurement of risk perception as a mediator between user trust and their attitudes towards using the IoT. Data were collected from 387 respondents and were analysed using SPSS 25 and AMOS 25 statistics software. Exploratory and confirmatory analysis and structural equation modelling were applied. The findings showed that levels of security, privacy and familiarity affected trustin the IoT. Furthermore, these levels of trust in the IoT were found to affect both users' perceptions of risk in, and their attitude towards, using the IoT. The users' risk perception partially mediated the relations between users' trustand their attitude regarding use of the IoT. The framework was supported and interpreted by 40 per cent of the variance in the attitude towards usingthe IoT in healthcare, while the mediator showed 47 per cent of the variance in the attitude towards using the IoT inhealthcare.

INDEX TERMS Security, privacy, familiarity, trust, riskperception, healthcare, Internet of Things (IoT).

I. INTRODUCTION

The main support of change in most business processes is technology-driven innovation [1]. Among recent advanced technologies, the Internet of Things (IoT) has become a critical part of that support as companies build digital transformation into their processes and business models to enhance their competitive advantage. The IoT refers to a network of devices that contain electronics, sensors or software, and this enables them to connect at anytime and anywhere through a cyber-physical system [2], [3]. However, the potential of the IoT stretches beyond improvement of business strategies to the empowerment of employees through delegation of responsibilities, and to the personalisation of user services [4].

The potential effect of the IoT on society and the economy has increased due to the massive changes it heralds [3]. It is estimated that by 2030 there will be more than 500 billion devices connected to the Internet [4]. Global expenditure on the IoT reached US$772.5 million in 2018 and is forecast to surpass US$1 billion by 2020, reaching US$1.1 billion by 2021.

A global survey in 2018 that comprised 300 respondents from each of Brazil, France, Germany, Japan and the UK, and 500 respondents from each of the US and China, asked what

The associate editor coordinating the review of this article and approving it for publication was Mahmoud Barhamgi.

the participants expected of their IoT experience by 2030. Among the responses were expectations that the IoT would play a part throughout the respondents' daily lives, from waking them to offering help with reading or listening to the news based on their chosen headlines, through preparation of a suggested menu for the day based on the contents of the refrigerator, to control of heating or air-conditioning to save energy in homes and workplaces, managing and prioritising urgent emails, reserving car parking spaces and turning on the computer before the respondents arrived at the work place, and organising shopping with completion of the purchase involved. Ofthe participants, 71 per cent believed that the IoT had the potential to improve their lives, while 79 per cent of them would like to use the IoT both inside and outside the home. From a healthcare perspective, they also expected the IoT to provide daily recommendations of what they should eat, remind them regarding any medicines they should take, and propose sport or exercise they should undertake to improve their wellbeing, taking into consideration their daily schedules and their health conditions [5].

Some healthcare providers already use IoT applications to provide important medical services such as: embedded context prediction; embedded gateway configuration; indirect emergency treatment; semantic medical access; wearable device access; health information regarding children; community healthcare; and adverse drug reactions. Beneficiaries of this information can receive these services using various medical IoT applications, such as: healthcare solutions that use smart phones, wheelchair and medication management; rehabilitation systems; and systems to monitor oxygen saturation, body temperature, blood pressure and electrocardiograms; and sensing of blood glucose level [6]. Use of these IoT applications can reduce medical services' costs, improve the users' experiences and serve more patients with the limited availability of healthcare resources.

To prepare people for, and provide people with, personalised services, healthcare providers and associated businesses require authentication for online transactions. However, these transactions are risky for both service providers and users. Thus, users' behavioural patterns should be considered to authenticate them securely when delivering online services. However, information technology can be used to build and maintain continuous behavioural biometrics, which in turn can be utilised to create seamless, personalised, and secure user experiences that can lead to silent authentication in which the IoT is the main technology used for this purpose [7]. Concerns regarding security and privacy have grown with increasing use of the IoT [4], and this trend is expected to continue. Users fear that their personal data is not protected adequately, especially because unauthorised parties may monitor their devices. This reflects the crucial importance of IoT security [5]. Service providers can lose the trust of their users if they do not consider ways to reduce this anxiety or/and maintain insufficient privacy tools to protect their users' data. Karahoca, Karahoca, and Aksözinvestigated the differences between male and female users regarding their intentions to adopt the IoT in healthcare [8]. Their results suggested that for males, the perceived advantages of using the IoT were the main influence on the perceived ease of use, while for women, the ability to test the system and compatibility with their lifestyles had greater influence on the perceived ease of use [8]. Yet their study was limited to one factor while missing other important social and technological factors. Behavioural reasoning theory suggests that users' adoption of IoT-based wearables will be increased if the reasons for and against their use have been embedded in the marketing strategy, along with the steps taken by companies to reduce the number and severity of anti-adoption factors [9]. Another study by L. Gao and X. Bai examined the factors that affected consumers' adoption of the IoT by testing a Technology Acceptance Model (TAM) that combined three constructs. These were: individual characteristics of consumers (perceived behavioural control and perceived enjoyment); factors linked to the technology (trust in the system, perceived usefulness, and perceived ease of use); and social influence. The study concluded that trust in the technology was the key factor affecting consumers' intention to adopt the IoT. The findings also revealed that perceived psychological effects influenced consumers' interest in using the IoT, while their assessment and experience of the use of the IoT offset the perceived privacy risk [10].

These researchers used only experience theory and the TAM to examine the users' general experiences in the use of the IoT, but discoveringtheusers' acceptance of the use of IoT systems in healthcare was limited [11]. Thus, there is a need to explore the end users' perspective regarding the adoption of IoT technologies in healthcare services. The current study delves further into this subject and adds support factors such as familiarity with the technology, risk perception, and the attitude towardsusing IoT to provide more holistic overview forusers' willingness to adopt IoT when receiving healthcare services. The main aim of this study is to discover the influence of security, privacy, familiarity, trust, and risk perception on Omani users' attitudes towards the use of IoT technologies to receive healthcare services. The outcomes of this research will deliver a thorough understanding of how levels of security, privacy and familiarity affect users' trust in the IoT, and how trust can affect users' attitudes towards using IoT technologies. In addition, it will measure the ways in which risk perception can mediate in the relationship between the users' trust and their attitudes. Consequently, the findings will recommend ways in which IoT technology producers and IoT-based healthcare providers should either improve the security and privacy levels embedded in their IoT devices and applications, or/and prepare awareness programmes that can teach methods of safe use of the IoT and reduce risk perception.

II. USE OF INTERNET OF THINGS IN HEALTHCARE AND THE STUDY FRAMEWORK

The Internet of Things (IoT) has become a new buzz phrase in industry and academia. It has many applications in numerous fields including healthcare and medicine. However, most of the current research into the use of the IoT in healthcare has focused on the technical requirements and devices of the IoT and ways in which the connectivity and performance can be improved using the IoT. For example, in 2017 Park, Park, and Lee proposed a remote IoT monitoring system for patients at home [12]. The system was constructed and evaluated by running several experiments showing that the system had performed effectively, and that the protocol conversion process had functioned efficiently for the IoT environment. Another study conducted by Li and Pan suggested a physiological monitoring system for patients using the IoT [13]. It encompassed physiological multi-parameter measurement of vital signs using a smart mobile device, online analysis and emergency detection. All sensors and microprocessors in this system were integrated into one device. The smart phone played a key role in connecting the patient to the telemedicine center.These studies defined the technical elements of the IoT that would improve service quality [12], [13] but they did not consider the processing of the data.

Rathore, Paul, Ahmad, Anisetti, and Jeon suggested an intelligent care system relied on IoT-based sharing big data among all the devices in a healthcare system [14]. This system has advanced tools and features for collection of data generated by connected devices to the network. In this system, the collected data through various sensors could be attached to a user's body (such as wearable devices) to measure health parameters which would be conveyed to a primary mobile device. The collected data would then be submitted through the Internet to a main station where the data would be fully analysed to identify whether something wrong related to health conditions is going on or not.

In the same vein, Rathore, Ahmad, Paul, Wan, and Zhang proposed a real-time medical-emergency response system involving IoT-based medical sensors deployed on a user's body while data analysis was responsible for the analysis and decision making [15]. The system was evaluated successfully for its feasibility and efficiency using an UBUNTU 14.04 LTS core TMi machine.

These scholars emphasised the importance of the technical requirements of the IoT and ways in which healthcare data could be analysed. However, they did not examine how the system could be designed or provide any suggested architectures or approaches for the adoption of the IoT in the healthcare discipline. The design methodologies presented were not suitable from a designer's perspective, and did not consider the requirements of the contractor or the potential user. This aspect would require consideration of multifarious constraints, including the system lifetime, energy usage, comfort of use and even the price [16].

Javdani and Kashanian in 2018 investigated the application of the IoT in medicine with a service-oriented and security approach [17]. The researchers compared previous studies on the use of the IoT in healthcare systems and concluded that service-oriented architecture offered many benefits such as: wearable devices for smart healthcare; efficient use of limited resources; Cloud-based storage and transmission of medical data and images; wireless health monitoring; ubiquitous electronic healthcare; and systems that could accommodate the weak and elderly people. Since then, more emphasis has been placed on the use of service-oriented architecture in the IoT.

Regarding the user needs, Prayoga and Abraham investigated variables that could predict a potential user's intention to utilise an IoT health device, and integrated them into a theoretical model [18]. They analysed users' approval of the technology through a TAM, using perceived usefulness as the main predictor for behavioural intention. They integrated personality traits and facilitated appropriation as factors to determine perceived usefulness, and used the cultural-value orientations at the individual level to determine the antecedents of facilitated appropriation. The researchers found that the users' intentions to use the IoT as part of a health device depended on their perception of the device's usefulness.

Dziak et al. [16] considered an IoT-based home-care information system for indoor and outdoor use by the elderly individuals. The researchers suggested the use of the following technologies for localisation of the signals: radio-frequency identification (RFID), Wi-Fi, Bluetooth, the global positioning system (GPS) or the global system for mobile communications (GSM). Technologies suggested for the recognition of activity and behaviour classification involved artificial intelligence and machine-learning algorithms with an accelerometer, while monitoring of vital signs required use of an electrocardiogram. An inter-integrated circuit was used for control.

None of the above studies focused on security and privacy issues linked with the use of the IoT in healthcare, although some [19], [20] discussed the significance of these issues in the IoT environment. Various researchers have discussed other security-related concerns, such as that by Riazul Islam et al. [6] which threw light on the issue of accessibility of the wireless network to third parties [6]. Jing et al. [21] explained common security and privacy issues in denial of service attacks on the wireless IoT, forgery/middle attacks, and heterogeneous-network attacks. The researchers suggested that an IoT environment was more vulnerable to security issues than was a traditional network. Improvements were suggested, including: use of light-touch security solutions such as key management, access authentication and access control; and the imposition of a division between applications that required different computation complexities and different security levels.

Pulkkis, Karlsson, Westerlund and Tana discussed security, and privacy in an IoT-based system in the context of the implementation of the general data protection regulation issued by the European Union.According to the researchers, the data generated by the sensors needed to be reliable and correct to conform to the legislation. Meta data should be recorded that described the rights of access to the data source and the justification for storing such information. In addition to these IoT security requirements, healthcare applications were required to protect the privacy of users and provide practically fault-free reliability to safeguard the users [19].

Baek et al. [22] advised that a m-healthcare system which relied on IoT should have enhanced privacy by ensuring anonymous connection among the patient and the medical staff. To achieve data privacy and system security, the researchers proposed that aliases be put in place to facilitate the transfer of patients' biometric data and anonymous communication. This system would prevent linkage between stored data and users by a malicious Coud provider. Every message in every communication step would be encrypted to prevent eavesdropping.

Roman, Zhou and Lopez discussed the benefits and challenges of security, privacy and reliability in the case of the distributed IoT. The researchers reported that a distributed system showed many advantages over a centralised system with regard to privacy and data management, as the data was not generated, processed or stored at a single location. However, security still posed a challenge in regard to issues such as complex identification and authentication. Security could be improved through separate policies regarding access control, identification of unknown peers, complexity and flexible governance. Wide availability of service providers would improve reliability, ensuring that if one service provider failed, the system would use another entity that managed a similar data set. However, the performance could deteriorate because of data exchanges between different service providers [20].

To the best of our knowledge, no study has examined the ways in which security, privacy and familiarity can affect trust in the IoT, and in turn how trust can affect risk perception and attitudes towards using the IoT. In addition, no research has considered ways in which risk perception can mediate in and perhaps strengthen the relationship between trust in the IoT and the users' attitudes towards using IoT in the healthcare area. Therefore, this study will shed light on this important aspect of use of the IoT in the healthcare sector by developing a framework to measure the causes and effects of these contingency factors, and how they can influence users' attitudes towards using the IoT in the health sector. In the next section, these factors are discussed in more detail to pave the way for developing the conceptual framework.

A. SECURITY

Security can be defined as the protection of resource hardware and software from damage, disruption, misdirection, misuse, malfunction or unauthorised access. As most IoT devices are wireless, this poses many security challenges such as intrusion, denial of service, forgery or heterogeneous network attack [6], [20], [21], [23]–[25]. These systems are also vulnerable to physical attack and damage [2], [26]. Many researchers [26]–[29] have offered several solutions to these security challenges such as use of intrusion detection, cryptography and stenography. Roman et al. [30] and Mahalle et al. [31] also recommended the use of personal identification and authentication, identification of malicious activities and similar functions to avoid such risks.

Moreover, Albalawi and Joshi showed the relationship between trust and security in their work [32]. The authors discussed a design solution at system level that would offer security and flexibility of the IoT. They proposed that to ensure the management of privacy and the secure operation of the system the functional components should be engaged in a security function group. They observed that, since CP-ABE was delegated to not restricted devices with the proposition that these devices were trusted, the producer encrypted the data. Data was protected through symmetric key solutions and the use of the advanced encryption standard (AES) and attribute-based encryption (ABE) schemes.

B. PRIVACY

The Merriam-Webster dictionary defines privacy as freedom from unauthorised intrusion. Privacy is an important challenge in the IoT environment, due to availability of sensory devices, and the speed and volume of information flow [33]. Any compromise of privacy may lead to problems such as eavesdropping [34], [35], unauthorised access to, or alteration or destruction of, information [36], hacking, identity theft, forgery and social engineering [37]. Some organisations are reluctant to adopt the IoT because of fears of privacy compromises [38], [39], particularly in cases that involve medical data, in which maintaining the privacy and anonymity of the user is of the utmost importance [22], [40]–[42] because of legal and statutory requirements, which in turn affect trust to adopt the IoT in the healthcare domain.

C. FAMILIARITY

Familiarity, according to the Cambridge dictionary, means good knowledge of some fact, or an understanding based on previous interactions [43]. Work by Gefen [44]showed the importance of familiarity and trust in an e-commerce prospective.Also,Komiak and Benbasat [45] argued that familiarity had an indirect positive influence on the intention to adopt recommended agents. Use of familiar features also increased product acceptance, usage and adoption [46].

D. TRUST IN IoT

Farahani *et al.* [47] in 2018 used a conventional trust framework to discuss security in mobile networks as the key anchor of IoT trust in terms of monitoring of device behaviours, device identification, connection protocols and the connection process to devices. Security measures at device level, could be adopted to enhance security. At the network level, security could be improved by using point-to-point encryption techniques based on cryptographic algorithms, message integrity verification techniques, and trusted routing mechanisms. The research reported that security measures to prevent data security and privacy were required to be adopted at Cloud level, and appropriate training regarding awareness was needed at human level.

The heterogeneity and dynamicity in IoT systems lead to difficulties in ensuring a build-up of trust during use of the IoT. Ferraris et al. [48] proposed a design of a trust framework and suggested that trust be included in the development of any IoT entity, taking into consideration all the phases of the system life-cycle. They concluded that trust in the IoT system lifecycle was necessary to guarantee delivery of a good service for the entire system. Bao and Chen developed a dynamic protocol for trust management which enables IoT systems to deal with misbehaving nodes whose status or behaviour might change dynamically. The proposed protocol was capable of adaptively and dynamically adjusting the best trust parameter settings to maximise the application performance [49].

Another study, by Kotis and Vouros [50] presented an extensible trust model that was seamlessly integrated into the IoT ontology. The authors focused on IoT-trust modelling, reusing existing trust models and ontology as well as a framework for fuzzy semantics. The Kotis and Vouros model showed through semantics that it could enable trust in the IoT and ensure effective deployment in many contexts. Machara, Chabridon, and Taconet, in their work, designed meta-models for contractors by defining privacy and quality-of-context conventions independently from those of the users and the creators. The convenes were the key to the independent management of quality-of-context and privacy in the IoT. However, these convenes would contribute to the building of trust among all IoT participants [51].

Using a different method, Gu et al. [52] established a formal trust-management control mechanism based on the architecture modelling of the IoT. The authors deconstructed the IoT into three layers: the sensor, core and application layers. Each layer was controlled by separate sets of trust management for self-organisation, effective routing and multi-service tools respectively. The final decision-making was performed by a service requester according to the collected trust information and the requester's policy. To realise all these trust mechanisms, the authors used formal semantics-based and fuzzy theory. The result was the production of a general framework for development of trust models for the IoT [52]. However, Leister and Schulzcriticised the complicated nature of the framework, stating that the composition of nodes and channels to complex networks was a challenge in itself. The lack of consideration of trust in relation to the quality of experience (QoE) was also seen as a shortcoming. This relates to the user experiences of a service and the authors stated that it should be considered in the framework [53].

Distrust of information technology can increase if a result arrives later than expected or is inaccurate. Fernandez-Gago et al. [54] introduced a framework to assist developers by involving trust in IoT scenarios, taking in consideration identity and privacy requirements to provide different services that allowed the inclusion of trust in the IoT.

One of the important challenges regarding trust in the IoT is the establishment of remote IoT devices. This is typically achieved by performing a distant ratification [55]. The researcher argued that most of the surveyed attestation techniques, from the perspective of IoT devices had a role to play in the establishment of trust in the IoT.

E. RISK PERCEPTION

Risk perception is the subjective judgment that people make about the characteristics and severity of a risk. Asplund and Tehrani [56] in a survey found that respondents were not in consensus regarding the perception of risk. Many researchers found that perceived risk influenced consumers' online behaviour [57]–[60]. Jalali *et al.* [61] concluded that the perceived risk was a major obstacle in IoT adoption. Li [62] studied risk perception among users of smart devices linked to the IoT at home and found that the risk perception was associated with knowledge of and anxiety regarding the devices. Hsu and Lin [63] also reported that risk perception was a key factor in determining IoT adoption. Regarding user needs,AlHogail and AlShahrani stated that trust was crucial when adopting IoT to ensure satisfactory and expected transaction results. The authors developed a conceptual model for trust that contained the main constructs influencing trust towards the adoption of IoT technology: three domain product-related factors, social influence-related factors such as the consumer's social network and community interest, and security-related factors such as security of product or services and perceived risk of product or services. Its design was based on the theory of the TAM. Their findings indicated that trust in the IoT affected positively the users' perception of risk and uncertainty, and it enhanced the users' acceptance of the technology that then had a positive impact on the intention to adopt the IoT. [64].

F. ATTITUDE TOWARD USING IoT

Attitude can be defined as afeeling or opinion regarding something or someone, or a way of behaving that is caused by something or someone. Achituv and Haiman [65] found that doctors held positive attitudes towards IoT-based medical devices, which meant that they were aware of and ready to use this technology. Kim [66] found that most IoT users show a positive attitude towards using IoT devices, and ascribe a greater quality to the information transmitted. Liu *et al.* [67] reported that most users of the IoT in healthcare held positive views regarding valuable functions and preferred solutions in areas such as inventory or material tracking, and identification and authentication that could make healthcare services more effective, convenient and safe. Barsaum *et al.* [68] found that even patients held favourable views towards using IoT devices.

Accordingly, the theoretical framework for this study was designed to reflect the literature discussed above. It is shown in Figure 1.

The hypotheses that were developed from this theoretical framework were:

H1: Security has a positive effect on trust in the IoT.

H2: Privacy has a positive effect on trust in the IoT.

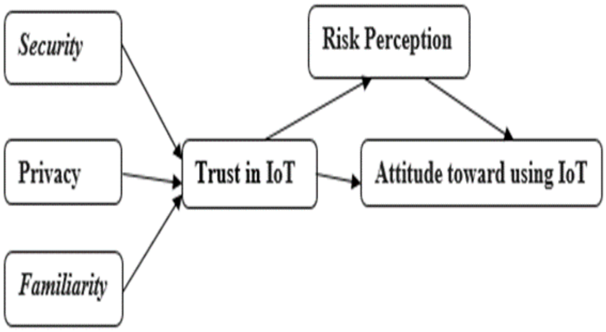

FIGURE 1. Theoretical framework.

H3: Familiarity has a positive effect on trust in the IoT.

H4: Trust positively affects the attitude toward using the IoT

H5: Trust in the IoT has a positive effect on risk perception.

H6: Risk perception has a positive effect on the attitude towards using the IoT.

H7: Risk perception mediates in the relationship between trust in the IoT and users' attitude towards using the IoT.

III. METHODOLOGY

The population of the research included all residents of Oman, whether as citizens or expatriates, aged between 18 years and 60 years. The population of Oman was stated in NCSI in 2018 to be 4,654,722. Of this number, 55.9 per cent were Omani while the other 44.1 per cent were expatriates [69]. However, this study targeted only owners of smart phones which had an available Internet connection. A paper-based survey was adopted from a previously validated instrument to collect primary data for the study. This survey was then adapted for an Omani context by adding a few questions. Five members of the college of commerce and business administration at Dhofar University, two of whom had authored publications related to the IoT, reviewed the first draft of the questionnaire to ensure that the questions were understandable, readable and appropriate in the context of the study. The questionnaire was required to be distributed to Arabic speakers, and therefore, copies were translated from English into Arabic. Two bilingual faculty members checked and reviewed both the English and Arabic questionnaires. Afterwards, a pilot study was conducted at Dhofar University among part-time students studying commerce and business administration. Most of these students are employees with an average age of 30 years. The feedback from the pilot study was utilised to modify the final survey.

To ensure confidentiality, all respondents were asked to sign consent forms that explained the purpose of the study and contained a guide regarding ways to answer the questions. An ethics form was provided which assured respondents of their anonymity when completing the questionnaire, and explained how the data would be stored and for how long, how it would be processed and how it would be destroyed at the end of the study.

This study used the following previously validated instruments: 1) The security and reliability items adapted from previous work [70]–[73]; 2) The privacy items adapted from former studies [71], [72]; 3) The familiarity items adapted from [44]; 4) The risk perception items adapted from [71]; 5) The items related to trust in the IoT adapted from [73]; and 6) The measurement of attitude towards using the IoT adapted from [44].

Five hundred respondents were targeted. They were required to own a smart device (smart phone, tablet or I pad) with Internet access and a medical account in the national medical system that is adopted in Oman. A non-probability and convenient sampling method was used to target the respondents, and all were selected on the basis of their accessibility. All questionnaires were distributed in the Dhofar Governorate which is the second-largest governorate in Oman after Muscat Governorate (the capital of Oman) in term of population.

Of the 500 questionnaires distributed,426 were returned, with 39 of these rejected as they were not completed, did not comply with the research conditions, or all questions were given the same answer. Then, 387 valid questionnaires, or 77.4 per cent of those distributed, were analysed using the statistical analysis software SPSS 25 and AMOS 25. Exploratory and confirmatory analysis was applied for the purpose of validating the instrument, while the hypotheses were tested using the structural equation modeling.The following sections explain these instruments and how they were applied in this study.

IV. DATA ANALYSIS AND RESULTS

A. EXPLORATORY STUDY

To remove any insignificant items from the adapted scale, the study implemented the corrected item-total correlation (CITC) analysis. Consequently, all the items of the study scale exceeded the accepted threshold value of 0.30 [74], [75]. Removing items that fall outside this value helps to refine the dataset and reduce the probability of it affecting the outcome of the exploratory factor analysis. The result of the Skewness and Kurtosis statistical test for each construct was between +2 and −2 [76], showing that the responses regarding the study's constructs were normally distributed. Furthermore, the Cronbach's alpha shown in Table (2) indicate that all the constructs were above the acceptable level of 0.70 [77].

To identify whether exploratory factor analysis (EFA) was suitable for the collected data, the authors of this study conducted Bartlett's test of sphericity and the Kaiser-Meyer-Oklin (KMO) test of sampling adequacy. The value of Bartlett's test of sphericity was less than 0.001, and the KMO value was greater than 0.60, which meant that the EFA was suitable for use with the collected data [78].

Furthermore, the results of the EFA using the principal component analysis with varimax rotation showed that the loadings of the measured items on their linked factors were greater than 0.40 [79]. Therefore, these results confirmed that EFA was suitable for the collected data.

TABLE 1. KMO and bartlett's test.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.828a
Bartlett's Test of Sphericity	Approx. Chi-Square	3666.937
	Df	276
	Sig.	0.000

TABLE 2. Descriptive analysis and EFA factor loadings.

Constructs	Items	Mean	Std. D	CITC	Skew	Kurtosis	α	Factor loadings
Security (Sec)	scu1	3.96	0.85	.630	-0.69	-0.21	0.80	0.77
	scu2			.524				0.80
	scu3			.597				0.80
Privacy (Pri)	pri1	3.75	0.84	.625	-0.07	-0.77	0.86	0.80
	pri2			.634				0.82
	pri3			.693				0.82
Familiarity (Fam)	fam1	3.71	0.81	.672	0.17	-0.86	0.71	0.55
	fam2			.709				0.57
	fam3			.461				0.47
Trust (Tru)	tru1	3.73	0.83	.690	0.20	-0.78	0.81	0.70
	tru2			.721				0.53
	tru3			.733				0.68
Perceived Risk (PR)	ris1	3.65	0.83	.706	0.33	-0.91	0.82	0.58
	ris2			.718				0.75
	ris3			.710				0.81
Attitude Toward Using IoT (ATUIoT)	atu1	3.72	0.81	.689	-0.03	-0.19	0.80	0.57
	atu2			.691				0.51
	atu3			.734				0.73

To check whether the common method bias was detected in this study, all the items were loaded into one common factor using Harman's single factor score. From the data in Table (3), it can be seen that the total variance for a single factor was less than 50 per cent [80], which means the common method bias had no effect on the collected data.

TABLE 3. One factor model (CMV).

Component	Initial Eigen values			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.99	49.9	49.9	8.996	49.9	49.9
2						
17						
18	.23	1.27	100			
Note: Extraction Method: Principal Component Analysis.						

B. CONFIRMATORY STUDY

Following the first set of analyses using EFA, the confirmatory factor analysis (CFA) was applied. To determine how well the number of constructs was represented by the measured variables, the fit indices of a confirmatory model were applied. Table (4) shows that all fit indices were within the acceptable range.

TABLE 4. Fit indices of confirmatory model.

fit indices	*Recommended*	*Measured*
X2/df	$2< X^2/df<5$	*3.028*
GFI	*>0.90*	*0.91*
CFI	*>0.90*	*0.94*
IFI	*>0.90*	*0.914*
TLI	*>0.90*	*0.924*
RMR	*<0.08*	*0.039*
SRMR	*<0.08*	*0.041*
RMSEA	*<0.08*	*0.07*

Table (5) presents the results of the CFA, which shows how the convergent validity has been determined [81]. The composite reliability of all constructs registered more than 0.70, and this result was confirmed by the test of average variance explained (AVE). All constructs were within the acceptable level of 0.50 [82]–[84]. Moreover, all the values of standardised factor loadings exceeded the acceptable threshold of 0.50. Hence, the next step was to examine the discriminant validity.

To confirm the discriminant validity [85], [86], the Chi-square difference test was performed. Two models resulted: model 1 showed that the constructs were not correlated, while in model 2, all constructs were correlated to each other (see Figures 2 and 3). Thereafter, the Chi-square difference was calculated, as demonstrated in Table 6.

TABLE 5. Confirmatory factor analysis results.

#	Constructs	Items		Standardized Factor Loadings (St. FL>.50)	Square Multiple Correlations (SMC>.30)	CR >.70	AVE >.50
1	Security (Sec)	scu1		0.57	0.32	0.72	0.59
		scu 2		0.78	0.61		
		scu3		0.58	0.34		
2	Privacy (Pri)	pri1		0.64	0.41	0.86	0.67
		pri2		0.75	0.57		
		pri3		0.72	0.51		
3	Familiarity (Fam)	fam1		0.66	0.44	0.74	0.50
		fam2		0.81	0.66		
		fam3		0.69	0.47		
4	Trust (Tru)	tru1		0.66	0.44	0.82	0.60
		tru2		0.82	0.68		
		tru3		0.68	0.46		
5	Perceived Risk (PR)	ris1		0.81	0.65	0.82	0.60
		ris2		0.82	0.67		
		ris3		0.81	0.65		
6	Attitude Toward Using IoT (ATUIoT)	atu1		0.82	0.67	0.80	0.57
		atu2		0.75	0.57		
		atu3		0.83	0.69		

TABLE 6. Model 1 & 2 of Chi-square difference test.

Model 1: CFA, constructs are not corelate	Model 2: CFA, constructs are corelate
Chi-square = 1848.115 Degrees of freedom = 135 Probability level = .000	Chi-square = 363.382 Degrees of freedom = 120 Probability level = .000

This confirmed a significant level at p = 0.00 <0.05, which in turn determined the adequacy of the discriminant validity test.

C. TESTING THE STRUCTURAL MODEL

The proposed model of the study was examined using structural equation modeling (SEM) as presented in Figure 4.

The structural model illustrates a good fit as all the fit indices represented in Table (7) were within the recommended values. Hence, with acceptable fit indices, the last phase of the analysis could be performed, which was the hypotheses test.

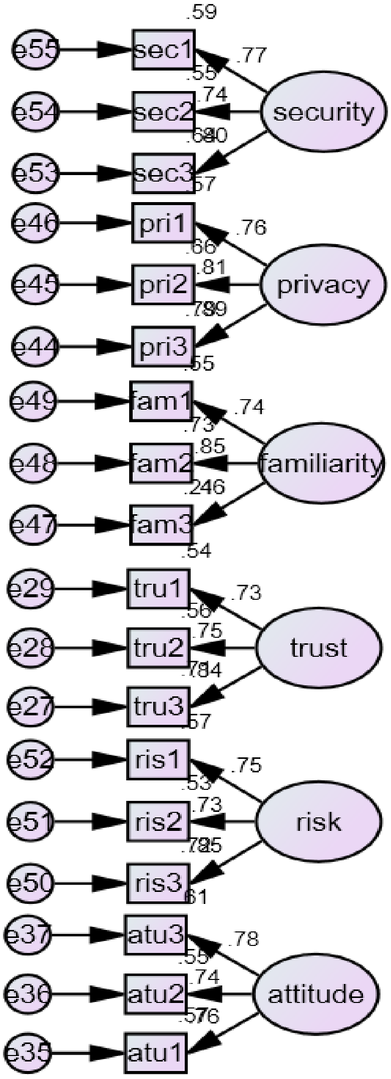

FIGURE 2. CFA, constructs are not correlate.

TABLE 7. Fit indices of structural model.

fit indices	*Recommended*	*Measured*
X2/df	$2< X^2/df<5$	*3.028*
GFI	*>0.90*	*0.904*
CFI	*>0.90*	*0.937*
IFI	*>0.90*	*0.91*
TLI	*>0.90*	*0.924*
RMR	*<0.08*	*0.040*
SRMR	*<0.08*	*0.042*
RMSEA	*<0.08*	*0.073*

The study hypotheses were tested using the structural model figures and by calculating the p-values with their standard regression weights. The results obtained from the structural model analysis are summarised in Table 8. The accepted and/or rejected hypotheses are shown. The results in Table 8 also revealed that security, privacy, and familiarity indicated standard regression weights of 0.21 (p = 0.01), 0.23 (p = 0.00), and 0.56 (p = 0.00) respectively, interpreting 20 per cent of variance in the amount of trust as a dependent variable. Trust in the IoT could be seen to show a positive effect on both attitudes towards the use of the IoT and the perceived risk, with standard regression weights of 0.40 (p = 0.00), and 0.92 (p = 0.00), correspondingly, with44 per

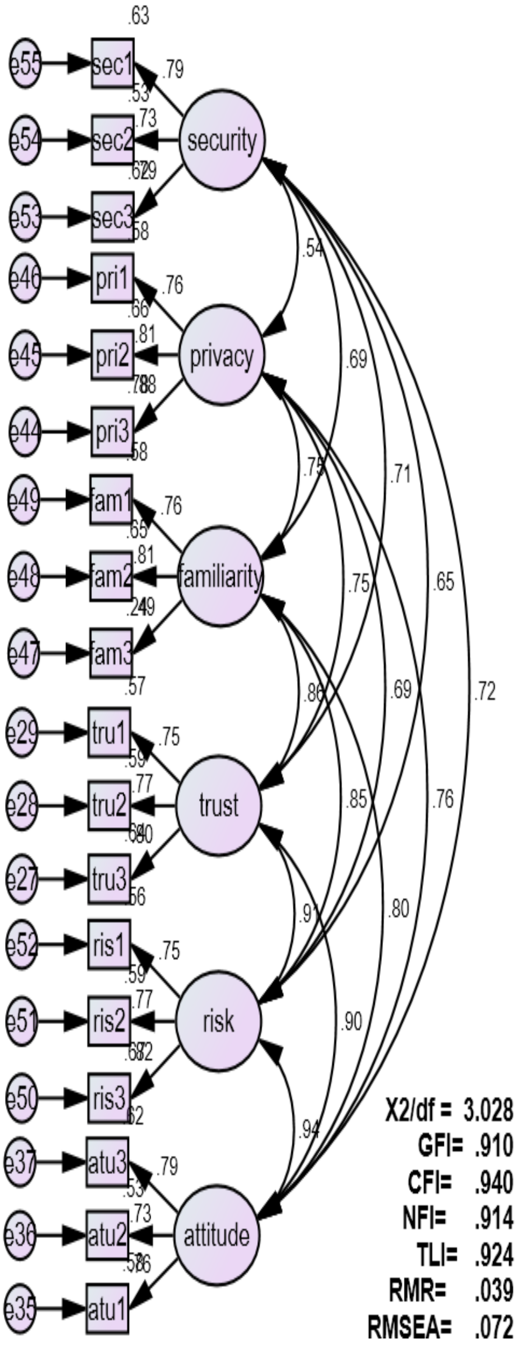

FIGURE 3. CFA, constructs are corelate.

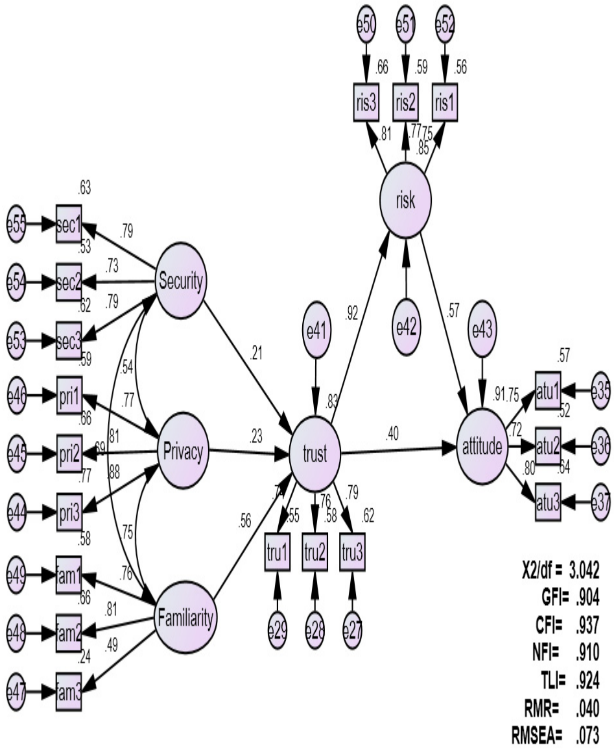

FIGURE 4. Tested model.

cent of the variance in the attitude towards using the IoT, and 26 per cent of the variance in the perceived risk.

However, the most interesting results of this study were that the perceived risk positively affected the attitude towards using the IoT, with standard regression weight of 0.57 ($p = 0.00$) explaining 57 per cent of the variance in the attitude towards using the IoT. Also, the perceived risk partially mediated the relation between trust and the attitude towards using the IoT, with standard regression weight of 0.47 ($p = 0.00$). The following section discusses the findings in more detail.

V. DISCUSSION AND IMPLICATIONS

This study aimed to understand users' attitudes towards the use of the IoT in the healthcare sector by adapting and extending prior work that involved rich conceptualisations of technology acceptance models. A model that examined the effect of a set of factors on attitudes toward the use of the IoT was developed based on previous studies. Five key contextual factors related to the acceptance of technology were determined and involved in this model. To validate the adapted model, a quantitative study was applied, which revealed that the model was supported and interpreted 40 per cent of the variance in the attitudes towards using the IoT in healthcare. The mediator explained 47 per cent of the variance in the attitudes toward using the IoT in the healthcare field.

A. THEORETICAL IMPLICATIONS

This work contributes to the body of knowledge in many ways. First, it contributes to the literature regarding acceptance of technology in general and particularly of the IoT. Whereas most prior studies have examined the technical aspects of the IoT and its use [87]–[94], this work extends the prior work by adapting a rich conceptualisation of IoT adoption and incorporating important technology acceptance factors with the aim of developing a better understanding of the user attitude towards using the IoT in the health sector.

Traditional statistical analysis in the form of regression analysis enables only the measurement of the causal relationship between the independent variables, such as security, privacy, and familiarity, and the dependent variables, such

TABLE 8. Results of hypothesis test.

S. No	Hypothesis	Direct effect	Indirect effect (the mediator)	Standard Regression Weights (SRW)	T-Value (TV> +2.33 or TV< - 2.33 for p<0,01)	Results
1	H1- security positively affects the trust	Sec → Tru	--	0.21	3.58 (p=0.00)	**Supported**
2	H2- Privacy positively affects the trust	Pri → Tru	--	0.23	3.44 (p=0.00)	**Supported**
3	H3- Familiarity positively affects the trust	Fam → Tru	--	0.56	5.40 (p=0.00)	**Supported**
4	H4- Trust positively affects the attitude toward using IoT	Tru → Atu	--	0.40	2.47 (p=0.01)	**Supported**
5	H5- Trust positively affects the perceived risk	Tru → PR	--	0.92	15.74 (p=0.00)	**Supported**
6	H6- Perceived risk positively affects the attitude toward using IoT	PR → Atu	--	0.57	3.37 (p=0.00)	**Supported**
7	H7- Perceived risk mediate the relation between trust and the attitude toward using IoT	--	Tru → PR → Atu	0.47	-- (p=0.04)	**Partially mediated**

as trust in the IoT or users' attitudes towards using the IoT. Yet no study has examined ways in which these factors can affect attitudes towards the use of the IoT, or whether any factor mediates in this relationship between two other factors. This paper addresses the challenges of implementing the IoT by integrating multilevel statistical analysis, starting with purification of the collected data and the removal of all insignificant items, and ending with a hypotheses test that uses the structural equation modelling method.

The study found that users' trust was likely to increase when users believed that no one could access their health data without their permission. This was especially the case if they had been protected through the use of various security measures put in place by healthcare providers. Moreover, users' trust in the use of IoT increased when the healthcare providers ensured that personal data would not be misused, and when they used modern technologies to protect the users' data from hacking. A positive correlation was found between user familiarity in using the new technologies, such as devices, applications and the Internet, and their trust in those technologies, and therefore they were more likely to use healthcare services provided through the IoT.

Further, high levels of certainty, reliability and guarantees offered through the IoT healthcare providers reduced the users' perception of the risks involved in use of the IoT and therefore improved their attitude towards using the IoT.

Another contribution of this study was the demonstration that risk perception mediates in and strengthens the relationship between trust in the IoT and users' attitude towards the use of the IoT. Therefore, this study shed light on another important aspect of IoT use in the healthcare sector.

By demonstrating the positive influence of security, privacy and familiarity on users' trust in the IoT, this work produced evidence of the importance of security, privacy, and familiarity to emphasise the effectiveness role of overall healthcare providers. This study also extended the research regarding digital transformation by extending such studies to the context of the IoT, and by developing a better understanding of ways in which risk perception mediated in the relationship between trust in the IoT and users' attitudes towards using the IoT.

Users' acceptance of information technology has been investigated in a wide range of prior research [95]–[101], but the users' attitudes towards the use of the IoT had not been adequately understood. Generally, the results of this research were in agreement with many previous findings. However, in some cases they were not in consonance with former studies: for example, in other studies, security was perceived to be the most critical factor affecting consumers' decisions to trust an IoT product [102]. Also, although some people were concerned about the consequences of safety and security [103], there was a significant effect but weak correlation between security awareness and adoption of the IoT [104]. Yildirim and Ali-Eldin [105] observed that privacy concerns regarding the collection of data did not have a significant effect on the behavioural intention of using a wearable device at the workplace. However, privacy was among the highest priorities of technology companies to ensure consumers' trust [102], and it was found that privacy worries caused a significant negative impact on consumers' intentions to use the IoT service [106], [107].

In the same context, previous experiences, or familiarity, were found to have strong positive influence on online consumers' trust [72], while any reduction in perceived risk also positively influenced the intention to use the IoT service.

Any negative effect of perceived risk was at a medium level, in line with the results from Yildirim and Ali-Eldin [105]. In other studies, respondents were reported to show less concern about perceived risks, and trust in the IoT showed a statistically significant positive relationship with users' intentions to adopt the IoT [105], [108]. In contrast, another study showed that trust was not a significant predictor of user acceptance of the use of IoT technologies [10].

B. PRACTICAL IMPLICATIONS

This paper sought to determine the factors that affected users' trust in the IoT to receive healthcare services, and how risk perception mediated in the relationship between users' trust and users' attitudes towards the use of the IoT. In this context and given this study's findings, healthcare providers need to focus on improving their IoT infrastructure in order to enhance their security and privacy levels. They should also pay more attention to their users' awareness of IoT use in general, and consider ways in which they can augment and sustain their clients' security and privacy. Additionally, motivating the public to use the IoT in the healthcare sector is a key aim for healthcare providers, and they could consider methods such as acknowledging or/and rewarding users for genuine reviews or for referring a healthcare provider's IoT app to other users.

Regarding familiarity with the IoT, healthcare providers could recruit well-known users who play critical roles in their communities, particularly through social media, train them on the use of the IoT in the healthcare sector, raise their awareness regarding the pros and cons of that use, and then present them as ambassadors to the target community.

The results indicated also that the influence of trust in the IoT on users' attitudes toward using it in the healthcare sector was stronger when the perception of the risks involved was small. This highlights the importance of risk perception and its effect on users 'attitudes toward using the IoT. Healthcare providers should reinforce awareness regarding the use of the IoT in the healthcare sector, and use legal methods such as cookies to track people who are likely to adopt the IoT for their healthcare services. To increase the potential of these methods, healthcare providers should maintain up-to-date records regarding potential IoT users to develop and manage good relationships with these users. Moreover, healthcare providers can prepare users by offering training on how to receive healthcare services through the IoT, with the emphasis on the high level of security, and on ways to check and maintain their privacy. This type of training would reduce risk perception and encourage users to adopt IoT tools.

VI. LIMITATIONS AND FUTURE RESEARCH

Despite the significant findings of this study, there were limitations which could be addressed in future research. First, this paper explored the attitude toward using IoT technologies to receive healthcare services. Future research may investigate the application of this model to other potential uses of the IoT such as in-house electricity control, remote control of the users' cars, and reserving car parking spaces.

Second, this study examined the users' attitudes only; actual usage behaviour of the IoT to receive healthcare services was not measured. This could be added into the model and would enable the addition of factors that considered outcomes of using IoT technology, such as the perceived value.

Third, this paper inspected the attitudes towards using the IoT in a developing economy, and the sample was selected from only one country. Future studies are advised to expand the study to cover the Gulf region. Additionally, the proposed model could be utilised in a comparative study to determine and compare users' attitudes in developing and developed economies.

Fourth, in this paper, a mediation role was embedded in the proposed model, yet other moderators such as the cultural dimension, gender and propensity to trust could be added to future research. Lastly, the study investigated the effect of levels of security and privacy without examining their components, or ways in which other factors might affect them. Therefore, future studies could investigate the main factors that affect security and privacy, thereby increasing users' acceptance of IoT technologies.

VII. CONCLUSION

The main purpose of this study was to investigate the impact of security, privacy and familiarity on users' trust in the IoT, and to explore the effect of trust on users' attitudes towards using IoT technologies to receive healthcare services. It also measured ways in which risk perception mediated in the relationship between user trust and attitudes towards using the IoT.

To validate an existing adapted instrument, exploratory and confirmatory analysis were applied, while structural equation modelling was applied to test the proposed hypotheses.

It was found that security, privacy and familiarity all affected the users' trust in the IoT in the healthcare area. Trust in the IoT was also affected by both the users' risk perception and their attitudes towards using the IoT. Finally, the level of risk perception was found to affect the users' attitudes and partially mediated in the relationship between users' trust and users' attitudes towards using the IoT.

This study contributes to literature regarding IoT adoption by developing a thorough understanding of ways in which security, privacy and familiarity affect user trust in the IoT, and how that trust affects user attitudes towards using IoT technologies. In addition, it measured how levels of risk perception mediated in the relations between the users' trust and their attitudes. Consequently, the findings recommended that IoT technology producers and IoT-based healthcare providers needed to improve the sophistication of the security and privacy embedded in their IoT devices and applications, or/and to design high-quality awareness programmes to teach the public ways in which they could use the IoT safely, and to reduce the users' perception of the risks of this technology.

REFERENCES

[1] S. Ammirato, F. Sofo, A. M. Felicetti, and C. Raso, "A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context," *Eur. J. Innov. Manag.*, vol. 22, no. 1, pp. 146–174, Jan. 2019.

[2] S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[3] X. Liang, "Internet of Things and its applications in libraries: A literature review," *Library Hi Tech*, Aug. 2018, pp. LHT-1–LHT-14.

[4] *Internet of Things: At-a-Glance*, CISCO, San Jose, CA, USA, 2016.

[5] *Connected Living: The Voice of the Consumer What do they Expect Their IoT Experience to be in 2030*, Gemalto, Amsterdam, The Netherlands, 2018.

[6] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[7] *Silent Authentication for a Fluid Consumer Experience*, Gemalto, Amsterdam, The Netherlands, 2018.

[8] A. Karahoca, D. Karahoca, and M. Aksöz, "Examining intention to adopt to Internet of Things in healthcare technology products," *Kybernetes*, vol. 47, no. 4, pp. 742–770, Apr. 2018.

[9] B. Sivathanu, "Adoption of Internet of Things (IOT) based wearables for healthcare of older adults—A behavioural reasoning theory (BRT) approach," *J. Enabling Technol.*, vol. 12, no. 4, pp. 169–185, Dec. 2018.

[10] L. Gao and X. Bai, "A unified perspective on the factors influencing consumer acceptance of Internet of Things technology," *Asia–Pacific J. Marketing Logistics*, vol. 26, no. 2, pp. 211–231, 2014.

[11] X. Dong, Y. Chang, Y. Wang, and J. Yan, "Understanding usage of Internet of Things (IOT) systems in China: Cognitive experience and affect experience as moderator," *Inf. Technol. People*, vol. 30, no. 1, pp. 117–138, Mar. 2017.

[12] K. Park, J. Park, and J. Lee, "An IoT system for remote monitoring of patients at home," *Appl. Sci.*, vol. 7, no. 3, p. 260, Mar. 2017.

[13] H. Li and T. Pan, "Development of physiological parameters monitoring system using the Internet of Things," *Int. J. Online Eng.*, vol. 13, no. 9, pp. 87–100, Jan. 2017.

[14] M. M. Rathore, A. Paul, A. Ahmad, M. Anisetti, and G. Jeon, "Hadoop-based intelligent care system (HICS): Analytical approach for big data in IoT," *ACM Trans. Internet Technol.*, vol. 18, no. 1, pp. 1–24, Dec. 2017.

[15] M. Rathore, A. Ahmad, A. Paul, J. Wan, and D. Zhang, "Real-time medical emergency response system: Exploiting IoT and big data for public health," *J. Med. Syst.*, vol. 40, no. 12, p. 283, 2016.

[16] D. Dziak, B. Jachimczyk, and W. J. Kulesza, "IoT-based information system for healthcare application: Design methodology approach," *Appl. Sci.*, vol. 7, no. 6, p. 596, Jun. 2017.

[17] H. Javdani and H. Kashanian, "Internet of Things in medical applications with a service-oriented and security approach: A survey," *Health Technol.*, vol. 8, nos. 1–2, pp. 39–50, May 2018.

[18] T. Prayoga and J. Abraham, "Behavioral intention to use IoT health device: The role of perceived usefulness, facilitated appropriation, big five personality traits, and cultural value orientations," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 4, pp. 1751–1765, Aug. 2016.

[19] G. Pulkkis, J. Karlsson, M. Westerlund, and J. Tana, "Secure and reliable Internet of Things systems for healthcare," in *Proc. IEEE 5th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2017, pp. 169–176.

[20] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[21] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[22] S. Baek, S.-H. Seo, and S. Kim, "Preserving patient's anonymity for mobile healthcare system in IoT environment," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 7, Jul. 2016, Art. no. 2171642.

[23] R. H. Waber, "Internet of Things: Privacy issues revisited," *Comput. Law Secur. Rev.*, vol. 31, no. 5, pp. 618–627, Oct. 2015.

[24] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015.

[25] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[26] T. Borgohain and U. Kumar, "A survey on security and privacy issues in Internet-of-Things," *Int. J. Adv. Netw. Appl.*, vol. 6, no. 4, pp. 2372–2378, Apr. 2015.

[27] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for Internet of Things: A study," *Int. J. Comput. Sci. Eng. Surv.*, vol. 2, no. 3, pp. 94–105, 2011.

[28] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things," *Comput. Elect. Eng.*, vol. 37, no. 2, pp. 147–159, 2011.

[29] T. Yan and Q. Wen, "A trust-third-party based key management protocol for secure mobile RFID service based on the Internet of Things," in *Knowledge Discovery and Data Mining*. Berlin, Germany: Springer, 2012, pp. 201–208.

[30] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011.

[31] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards Internet of Things (IoT): Roadmap and key challenges," in *Recent Trends in Network Security and Applications*, Berlin, Germany: Springer, 2010, pp. 430–439.

[32] U. Albalawi and S. Joshi, "Secure and trusted telemedicine in Internet of Things IoT," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 30–34.

[33] B. D. Weinberg, G. R. Milne, Y. G. Andonova, and F. M. Hajjat, "Internet of Things: Convenience vs. Privacy and secrecy," *Bus. Horiz.*, vol. 58, no. 6, pp. 615–624, Nov. 2015.

[34] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: A lightweight identity-based cryptography for body sensor networks," *Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 926–932, Jun. 2009.

[35] C. Huang, H. Lee, and D. H. Lee, "A privacy-strengthened scheme for E-healthcare monitoring system," *J. Med. Syst.*, vol. 36, no. 5, pp. 2959–2971, Oct. 2012.

[36] C. Sbora, "Indicators for determining collaborative security level in organizational environments," *Inform. Econ.*, vol. 18, no. 4, pp. 131–143, Dec. 2018.

[37] O. Osho and A. D. Onoja, "National cyber security policy and strategy of nigeria: A qualitative analysis," *Int. J. Cyber Criminol.*, vol. 9, no. 1, pp. 120–143, Jan. 2015.

[38] D. Kamin, *Exploring Security, Privacy, and Reliability Strategies to Enable the Adoption of IoT*. Minneapolis, MN, USA: Walden, 2017.

[39] H. Kim, J. Lim, and K. Lee, "A study of K-ISMS fault analysis for constructing secure Internet of Things service," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 9, Sep. 2015, Art. no. 474329.

[40] C. Humer and J. Finkle, "Your medical record is worth more to hackers than your credit card," Reuters, New York, NY, USA, Tech. Rep., 2014.

[41] H. Xu and F. Bélanger, "Information systems journal special issue on: Reframing privacy in a networked world," *Inf. Syst. J.*, vol. 23, no. 4, pp. 371–375, Jul. 2013.

[42] B. P. Rosenbaum, "Radio frequency identification (RFID) in health care: Privacy and security concerns limiting adoption," *J. Med. Syst.*, vol. 38, no. 3, p. 19, Mar. 2014.

[43] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. New York, NY, USA: Oxford, 2000, pp. 94–107.

[44] D. Gefen, "E-commerce: The role of familiarity and trust," *Omega*, vol. 28, no. 6, pp. 725–737, Dec. 2000.

[45] S. Y. X. Komiak and I. Benbasat, "The effects of personalization and familiarity on trust and adoption of recommendation agents," *MIS Quart.*, vol. 30, no. 4, p. 941, Dec. 2006.

[46] R. W. Proctor, T. Van Zandt, and T. Van Zandt, *Human Factors in Simple and Complex Systems*, 3rd ed. Boca Raton, FL, USA: CRC Press, 2018.

[47] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generat. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.

[48] D. Ferraris, C. Fernandez-Gago, and J. Lopez, "A trust-by-design framework for the Internet of Things," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–4.

[49] F. Bao and I.-R. Chen, "Dynamic trust management for Internet of Things applications," in *Proc. Int. Workshop Selfaware Internet Things*, vol. 2012, pp. 31–34.

[50] K. Kotis and G. A. Vouros, "Trust semantics in IoT entities,'Deployment," in *Proc. 9th Hellenic Conf. Artif. Intell. (SETN)*, Jul. 2016, pp. 1–6.

[51] S. Machara, S. Chabridon, and C. Taconet, "Trust-based context contract models for the Internet of Things," in *Proc. IEEE 10th Int. Conf. Ubiquitous Intell. Comput.*, Dec. 2013, pp. 557–562.

[52] G. Lize, W. Jingpei, and S. Bin, "Trust management mechanism for Internet of Things," *China Commun.*, vol. 11, no. 2, pp. 148–156, 2014.

[53] W. Leister and T. Schulz, "Ideas for a trust indicator in the Internet of Things," in *Proc. 1st Int. Conf. Smart Syst., Devices Technol.*, May 2012, pp. 1–9.

[54] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling trust dynamics in the Internet of Things," *Inf. Sci.*, vol. 396, pp. 72–82, Aug. 2017.

[55] T. Abera, "Invited—Things, trouble, trust: On building trust in IoT systems," in *Proc. 53rd Annu. Design Autom. Conf.*, Jun. 2016, pp. 1–6.

[56] M. Asplund and S. Nadjm-Tehrani, "Attitudes and perceptions of IoT security in critical societal services," *IEEE Access*, vol. 4, pp. 2130–2138, 2016.

[57] L. F. Cunningham, J. Gerlach, and M. D. Harper, "Perceived risk and e-banking services: An analysis from the perspective of the consumer," *J. Financ. Serv. Mark.*, vol. 10, no. 2, pp. 165–178, Nov. 2005.

[58] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *Int. J. Electron. Commer.*, vol. 7, no. 3, pp. 101–134, Apr. 2003.

[59] A. F. Salam, H. R. Rao, and C. C. Pegels, "Consumer-perceived risk in e-commerce transactions," *Commun. ACM*, vol. 46, no. 12, pp. 325–331, Dec. 2003.

[60] A. E. Schlosser, T. B. White, and S. M. Lloyd, "Converting Wab site visitors into buyers: How Wab site investment increases consumer trusting beliefs and online purchase intentions," *J. Mark.*, vol. 70, no. 2, pp. 133–148, Apr. 2006.

[61] M. S. Jalali, J. P. Kaiser, M. Siegel, and S. Madnick, "The Internet of Things (IoT) promises new benefits and risks: A systematic analysis of adoption dynamics of IoT products," *SSRN Electron. J.*, vol. 17, no. 2, pp. 39–78, Aug. 2017.

[62] L. Li, *An investigation on the Risk Perception of Residents in IoT Smart Home Environments*. Eindhoven, The Netherlands: Eindhoven Univ. Technol., 2017.

[63] C.-L. Hsu and J. C.-C. Lin, "Exploring factors affecting the adoption of Internet of Things services," *J. Comput. Inf. Syst.*, vol. 58, no. 1, pp. 49–57, Jan. 2018.

[64] A. AlHogail and M. AlShahrani, "Building consumer trust to improve Internet of Things (IoT) technology adoption," in *Advances in Neuroergonomics and Cognitive Engineering*, Cham, Switzerland: Springer, 2019, pp. 325–334.

[65] D. B. Achituv and L. Haiman, "Physician's attitudes toward the use of IoT medical devices as part of their practice," *Online J. Appl. Knowl. Manag.*, vol. 4, no. 2, pp. 128–145, 2016.

[66] K. J. Kim, "Interacting socially with the Internet of Things (IoT): Effects of source attribution and specialization in human—IoT interaction," *J. Comput. Commun.*, vol. 21, no. 6, pp. 420–435, Nov. 2016.

[67] L. Liu, W. P. Chen, A. Solanas, and A. L. He, "Knowledge, attitude, and practice about Internet of Things for healthcare," in *Proc. Int. Smart Cities Conf. (ISC2)*, Sep. 2017, pp. 1–4.

[68] P. Barsaum, P. Berg, A. Hagman, and I. Scandurra, "Internet of Things technology for remote healthcare—A pilot study," in *Proc. 14th Scandin. Conf. Health Informat.*, Mar. 2016, pp. 43–48.

[69] National Center for Science Information, (2018). *National Centre For Statistics Information*. Accessed: Oct. 26, 2018. [Online]. Available: https://www.ncsi.gov.om/Pages/NCSI.aspx

[70] S. M. Furnell, P. Bryant, and A. D. Phippen, "Assessing the security perceptions of personal Internet users," *Comput. Secur.*, vol. 26, no. 5, pp. 410–417, Aug. 2007.

[71] B. J. Corbitt, T. Thanasankit, and H. Yi, "Trust and e-commerce: A study of consumer perceptions," *Electron. Commer. Res. Appl.*, vol. 2, no. 3, pp. 203–215, Sep. 2003.

[72] R. Connolly and F. Bannister, "Factors influencing Irish consumers' trust in Internet shopping," *Manage. Res. News*, vol. 31, no. 5, pp. 339–358, Apr. 2008.

[73] C. Cheung and M. Lee, "Trust in Internet shopping: A proposed model and measurement instrument," *Proc. AMCIS*, Jan. 2000, p. 406.

[74] L. J. Anthony, *The Cambridge Dictionary of Statistics*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2002.

[75] A. Field, *Discovering Statistics Using SPSS*, 2nd ed. Thousand Oaks, CA, US: Sage Publications, Inc., 2005.

[76] A. S. Al-Adwan, M. Alrousan, A. Al-Soud, and H. Al-Yaseen, "Revealing the black box of shifting from electronic commerce to mobile commerce: The case of Jordan," *J. Theor. Appl. Electron. Commerce Res.*, vol. 14, no. 1, pp. 51–67, 2019.

[77] S. F. Wamba, A. Gunasekaran, S. Akter, S. J. Ren, R. Dubey, and S. J. Childe, "Big data analytics and firm performance: Effects of dynamic capabilities," *J. Bus. Res.*, vol. 70, pp. 356–365, Jan. 2017.

[78] S. Ambulkar, J. Blackhurst, and S. Grawe, "Firm's resilience to supply chain disruptions: Scale development and empirical examination," *J. Oper. Manag.*, vols. 33–34, pp. 111–122, Jan. 2015.

[79] Y. K. Dwivedi, J. Choudrie, and W. Brinkman, "Development of a survey instrument to examine consumer adoption of broadband," *Ind. Manag. Data Syst.*, vol. 106, no. 5, pp. 700–718, Jun. 2006.

[80] P. M. Podsakoff, S. B. MacKenzie, and N. P. Podsakoff, "Sources of method bias in social science research and recommendations on how to control It," *Annu. Rev. Psychol.*, vol. 63, no. 1, pp. 539–569, Jan. 2012.

[81] T. K. Chan, C. M. Cheung, N. Shi, and M. K. O. Lee, "Gender differences in satisfaction with Facebook users," *Ind. Manag. Data Syst.*, vol. 115, no. 1, pp. 182–206, Feb. 2015.

[82] R. P. Bagozzi and Y. Yi, "On the evaluation of structural equation models," *J. Acad. Marketing Sci.*, vol. 16, no. 1, pp. 74–94, 1988.

[83] J. Hulland, "Use of partial least squares (PLS) in strategic management research: A review of four recent studies," *Strategic Manage. J.*, vol. 20, no. 2, pp. 195–204, 1999.

[84] J. F. Hair, W. C. Black, and B. J. Babin, *Multivariate Data Analysis: A Global Perspective*. London, U.K.: Pearson Education, 2010.

[85] A. H. Segars, "Assessing the unidimensionality of measurement: A paradigm and illustration within the context of information systems research," *Omega*, vol. 25, no. 1, pp. 107–121, Feb. 1997.

[86] P. Bertea and A. Zait, "Methods for testing discriminant validity," *Manag. Mark.*, vol. 9, no. 2, pp. 217–224, Nov. 2011.

[87] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[88] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. L. Moullec, "A survey on the roles of communication technologies in IoT-based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36611–36631, 2018.

[89] A. I. E. S. Eldein, H. H. Ammar, and D. G. Dzielski, "Enterprise architecture of mobile healthcare for large crowd events," in *Proc. 6th Int. Conf. Inf. Commun. Technol. Accessibility (ICTA)*, Dec. 2017, pp. 1–6.

[90] N. L. Laplante, P. A. Laplante, and J. M. Voas, "Stakeholder identification and use case representation for Internet-of-Things applications in healthcare," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1589–1597, Jun. 2018.

[91] M. Rath and B. Pattanayak, "Technological improvement in modern health care applications using Internet of Things (IoT) and proposal of novel health care approach," *Int. J. Hum. Rights Healthc.*, vol. 12, no. 2, pp. 148–162, Oct. 2018.

[92] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, Mar. 2018.

[93] K. G. Srinivasa, B. J. Sowmya, A. Shikhar, R. Utkarsha, and A. Singh, "Data analytics assisted Internet of Things towards building intelligent healthcare monitoring systems: IoT for healthcare," *J. Organ. End User Comput.*, vol. 30, no. 4, pp. 83–103, Oct. 2018.

[94] T. Tekeste, H. Saleh, B. Mohammad, and M. Ismail, "Ultra-low power QRS detection and ECG compression architecture for IoT healthcare devices," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 66, no. 2, pp. 669–679, Feb. 2018.

[95] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quart.*, vol. 13, no. 3, pp. 319–340, 1989.

[96] R. Rauniar, G. Rawski, J. Yang, and B. Johnson, "Technology acceptance model (TAM) and social media usage: An empirical study on Facebook," *J. Enterp. Inf. Manag.*, vol. 27, no. 1, pp. 6–30, Feb. 2014.

[97] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quart.*, Vol. 27, no. 1, p. 51, 2003.

[98] M. N. Alraja, "The effect of social influence and facilitating conditions on e-government acceptance from the individual employees," *Polish J. Manage. Studies*, vol. 14, no. 2, 2016.

[99] A. Barua, P. Konana, A. B. Whinston, and F. Yin, "Assessing Internet enabled business value: An exploratory investigation," *MIS Quart.*, vol. 28, no. 4, pp. 585–620, 2004.

[100] C. L. Iacovou, I. Benbasat, and A. S. Dexter, "Electronic data interchange and small organizations: Adoption and impact of technology," *MIS Quart.*, vol. 19, no. 4, p. 465, Dec. 1995.

[101] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quart.*, vol. 27, no. 3, pp. 425–478, 2004.

[102] A. AlHogail, "Improving IoT technology adoption through improving consumer trust," *Technologies*, vol. 6, no. 3, p. 64, Jul. 2018.

[103] S. Kim and S. Kim, "User preference for an IoT healthcare application for lifestyle disease management," *Telecomm. Policy*, vol. 42, no. 4, pp. 304–314, May 2018.

[104] A. A. Harper, *The Impact of Consumer Security Awareness on Adopting the Internet of Things: A Correlational Study*. Minneapolis, MN, USA: Capella University, 2016.

[105] H. Yildirimand and A. M. T. Ali-Eldin, "Amodel for predicting user intention to use wearable IoT devices at the workplace," *J. King Saud Univ.-Comput. Inf. Sci.*, Mar. 2018.

[106] T. Kowatsch and W. Maass, "Critical privacy factors of Internet of Things services: An empirical investigation with domain experts," in *Knowledge and Technologies in Innovative Information Systems—MCIS* (Lecture Notes in Business Information Processing), vol. 129, H. Rahman, A. Mesquita, I. Ramos, and B. Pernici, Eds. Berlin, Germany: Springer, 2012, pp. 200–211.

[107] Y. Kim, Y. Park, and J. Choi, "A study on the adoption of IOT smart home service: Using value-based adoption model," *Total Quality Manage., Bus. Excellence*, vol. 28, nos. 9–10, pp. 1149–1165, Apr. 2017.

[108] K. Patil, "Retail adoption of Internet of Things: Applying TAM model," in *Proc. Int. Conf. Comput., Anal. Secur. Trends (CAST)*, Jul. 2016, pp. 404–409.

MANSOUR NASER ALRAJA received the Ph.D. degree in management information systems.

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, e-commerce, and the IoT. Since 2016, he has been the Chair of the AACSB accreditation committee. More, in 2018, he has been appointed as the Chair for the Department of MIS.

Dr. Alraja is a member of the Information Systems Audit and Control Association (ISACA).

MURTAZA MOHIUDDIN JUNAID FAROOQUE received the Ph.D. degree in computers application from Savitribai Phule Pune Universiity.

He is currently an Assistant Professor with the College of Commerce and Business Administration (CCBA), Dhofar University. He was the Co-Editor of the *Proceeding of National Conference in Data Mining* (NCDM 2011) and NCDM (2013). He was the co-author of a book named the *Problems and Prospects of Using Social Networking Sites by Students of Management Institutes* (Himalaya Publications, India). His areas of interests are machine learning, social networking, data science, and medical informatics. He is a member of the Association of Computer Machinery (ACM), the Computer Measurement Group (CMG), and the Data Science Association.

BASEL KHASHAB received the M.Sc. degree in business computing, the B.Sc. degree in business management, and the Ph.D. degree from the Henley Business School in Business Informatics and Systems, University of Reading. He was with the Henley Business School and the University of West London, before joining the Greenwich School of Management as a Lecturer in E-commerce (Digital Innovation and Creative Enterprise Department). He is currently a Senior Lecturer in project management with Northumbria University—London Campus. His areas of interests include digital marketing, virtual reality, customer relationship management (CRM), enterprise resource planning (ERP), design science methodology, and higher education technologies.