Determinants of user acceptance of wearable IoT devices

Salem Ali Suhlu1* and Syed Md. Faisal Ali Khan1

Abstract: The Internet of Things (IoT) has modified our daily lives. This study examines the relationship between behavioural intention towards adoption of IoT wearable devices (WIoT) in the context of social norms, privacy, security concerns, and trust. The current study consists of a review of the literature for constructing the theoretical framework of the study and subsequently, survey was conducted from 200 respondents from Saudi Arabia was conducted between 2020 and 2020. The statistical results illustrate that the proposed model fits well for the current study and conclude that perceived privacy risks and health awareness have a significant impact on the intention to adopt wearable devices, whereas the social norms have a negative effect on the privacy and security concerns towards the use of WiOT devices. The study also helps to improve the predictability of user intention to use IoT devices.

Subjects: Legal, Ethical & Social Aspects of IT; Management of IT; Computing & IT Security

Keywords: Privacy; security; social norms; trust; IoT; wearable; behavioural intention

1. Introduction

The Internet of Things (IoT) refers to the system of internet-connected and -interrelated smart devices which collect and transfer data over a wireless network without any human control. IoT represents a major technological advancement (Malina et al., 2016; Erişen & D T Pham (Reviewing editor), 2022). The IoT has changed the effectiveness and convenience of our daily lives. The technology provides solutions to improve services including healthcare and transportation (Tawalbeh et al., 2020, Ali, 2015; Erişen & D T Pham (Reviewing editor), 2022).

PUBLIC INTEREST STATEMENT

Wearable devices are electronic devices connected to the human body and designed to sense certain variables or assist the end-user with daily tasks. Spectacles, wristbands, strips, caps, exoskeletons, vests, clothing, wallets, independent sensors, and any other item that a person can wear are examples of wearable devices. The interconnectedness of devices and their various purposes and capabilities makes a compelling justification for guaranteeing the security of IoT devices to preserve users’ data and secrecy. As wearable IoT devices have real-time access to high levels of personal information, the security and privacy of these wearable devices become a central factor in the relevant technologies. This proliferation of IoT wearable devices also creates major privacy and security concerns. As the IoT-based devices are still in progress, their security and privacy features are not yet developed to the highest standards. A majority of IoT gadgets and systems come short of design aspects that facilitate superior security and privacy. Threats to IoT security can materialise at the various levels of an IoT information network, like the IoT device itself, the coordinator, the sensor bridge, the service level, and the controller. In addition to the above general concerns, wearable devices can also have some specific security and privacy issues. They remain significant issues because IoT wearable devices obtain personal data such as names, mobile numbers, and other personal information of users. These gadgets can also collect user-related activities whether they are indoors or outdoors, their number of steps, places that they visited, and certain health data. This paper examined different factors and their role on users acceptance.
Wearable IoT (WIoT) has changed personal computing into a new innovative horizon. Their sensors have the advantage of being collecting real-time data for monitoring human's everyday activities. They are used to track and diagnose certain diseases, and contact health care professionals if needed. For instance, the built-in sensors in wristwatch detect tremors in patients (Gubbi et al., 2013; Sharma et al., 2014). WiIoT technology has expanded significantly in recent years. According to the recent research, there is a growth of 78.4% in the market for wearable smart devices in the second half of 2014. The devices include “hearables” which are worn in the ear to provide real-time information to users (Ulanoff, 2014).

However, WiIoT devices have some limitations related to the fact that they need to work close to other computing devices to compensate for their short battery life, low power, and their short connection range (Gubbi et al., 2013; Sharma et al., 2014). There are also a variety of security and privacy challenges associated with the WiIoT devices that connect to a large number of sensors connected to all-in-one architectural design. Additionally, their operational manageability and their maintenance would inevitably lead to an increase in the vulnerability of the WiIoT technology. For example, in 2016, about 300,000 WiIoT video recorders attacked multiple social networks in different regions and brought down Twitter for about 2 hours (Zanella et al., 2014; Yan et al., 2014).

Hence, giving rise to social norms where people strict to their sense of duty or their fear from external sanctions. They provide the way people expect others to deal in certain contexts. Social norms give people a sense of belonging, acceptance, and security (Cislaghi & Heise, 2020). The relation between social norms and technology is a matter of concern for ethical use of data which is further explained by the hypothesis that user adoption of IoT is governed by social norms associated with it (McLeod, 2008, Markets, 2017; Greenberg et al., 1977; Martin et al., 2019).

The term privacy protection refers to the degree to which individuals think their personal stored data are not misused or shared without their prospective consent. Security is related to the belief that an individual's data is protected and secured (Chellappa & Sin, 2005; Levin, 2002). Also, people's trust in a device could be affected by the conception that users' awareness of the extent to which their close ties expect them to use the device and from the opinion of other relatives. All of these conceptions are related to their societal norms (Chen & Dibb, 2010).

Wearable devices collect significant amount of data and information that raise number of privacy concerns. Moreover, it is also not known where this information is achieved and what is being done with that data (Flaherty, 2014). On the contrary, many users adopt them for regular use, raising many societal concerns (Hamblen, 2015). Despite this, the use of wearable devices can cause multiple threats to user’s privacy. Thus, there is always a trade-off between risks associated with the use of such technology and perceived benefits.

In this study, the researcher mentioned issues by proposing a conceptual model that defines factors influencing users’ intention to use wearable devices at the workplace. This model provides an understanding of the different factors that influence users’ intention to use wearable devices at the workplace, namely, individuals’ privacy concerns regarding information and additional factors such as risk, trust, and perceived usefulness. The paper outlined in later sections presents a literature review followed by the proposed model, explaining the data collection and analysis overviewed and results concluding the paper, providing highlights on possible future work.

1.1. Objective of the study

The current research including the survey aims to study how different factors such as security, social norms, trust, and privacy related to the WiIoT technology affect behavioural intention. This research will provide answers to the following questions: What is the impact of security, social norms, trust, and privacy related to the WiIoT technology that affect behavioural intention? How to improve security and privacy in the WiIoT devices?
1.2. Significance of the study
The current research deals with a serious problem and it benefits the IoT users to choose a better secure wearable device that fits with their social norms. Also, this work encourages manufacturers to design new wearable devices with better security and privacy which consider respecting peoples’ social norms.

2. Literature review

2.1. Security and privacy concerns
Security and privacy are interlaced and used synonymously with each other. There are several issues and threats related to security towards WiIoT devices (Xue, 2019). The authors mentioned that security risks are the primary problem of users, as data of users could be hacked or stolen easily. Then, the authors offered some solutions to reduce the problem including their proposed cloud/edge-supported WiOT system where the lower layer (virtual machine) is generated from the Amazon Web Service (AWS), the middle layer (Raspberry Pi 4 hardware kit), and the top layer (the cloud). They also implemented security certificates to allow data transfer between these layers (Tawalbeh et al., 2020). Additionally, the authors of “Review on security and privacy concerns in the Internet of Things” focused on vulnerabilities of technology. They included web interface vulnerabilities, data storage challenges, device connection problems, and issues related to the cloud connection (N. Kumar et al., 2017).

Granjal et al. (2015) mentioned that security concerns were related to confidentiality of users, and data authenticity and integrity. They further analysed various security protocols to improve security and suggested a compressed security header to deal with the network layer. They also proposed a common group key for users and security gateways to improve application layer security (Granjal et al., 2015). Moreover, some experts highlighted the risk of physical threat for a person’s safety. If a consumer, for instance, carries sensors which cover their eyes in a certain way, that person may fall down and could harm him/herself (Habibipour et al., 2019).

Through the review of literature, several articles have mainly focused on the WiIoT privacy concerns that indicated privacy concerns (Y Lee et al., 2018). However, privacy concern is a serious problem of IoT. Yang et al. (2017) mentioned the issues related to authentication and user’s access control. Then, the authors classified IOT attacks into software, physical, encryption, and network (Yang et al., 2017). Habibipour et al. (2019) interviewed experts and users to examine social, and ethical issues in the WiIoT. The authors discovered that experts were concerned with the need for informed consent under privacy protection. Also, WiIoT could easily make cognitive or health problems more visible to people observing them from external source in form of WiIoT, and this will affect user’s confidentiality (Chakraborty et al.; Chakraborty et al.). For example, if someone places a camera around a person’s neck, everyone knows that that person has a specific problem. The majority of users were concerned with their privacy protection; they have limited control over their personal information and a fear of taking photos and recording videos without their prior permission. Some of the users were concerned with data stored in the cloud (Habibipour et al., 2019).

The privacy concerns seem worse than people expect. The study of Datta et al. (2018) among WiIoT users at workplace showed that employees are afraid of being tracked by their employers, the devices could lead to distractions and the device might record sensitive information about the workplace (Datta et al., 2018). Moreover, the study of Motti and Caine (2015) explored the privacy issues related to WiIoT devices based on comments from users. Customer concerns were different according to the type of data each device collects, stores, processes, and shares. However, they all shared some concerns related to embedded sensors, such as cameras and microphones captured data about nearby people, even without their awareness or consent, while other sensors, such as heart rate monitors and activity trackers, were considered by users as involved in fewer privacy concerns (Motti & Caine, 2015). Privacy concerns become a major problem, especially, when they
are aggravated by societal norms. Canhoto and Arp (2017) analysed the factors that significantly affect the use of WIoT devices, and they included user's social expectation from the device and social pressure from their relatives and friends (Canhoto and Arp, 2017).

2.2. Security concerns related to WIoT devices

Security in the WIoT devices represents a “wicked problem”, where a potential technology could result in unanticipated negative effects. Reports show the frequency of data vulnerability has risen significantly in the last few years. Hacking of WIoT devices could cause serious troubles. Hackers’ aims of infecting a WIoT apparatus may not only be used for spying or intruding, they could also demand ransom money. Additionally, hackers may gain access to sensitive data and can use it against the owner. On the industrial level, a company’s data could be collected by hackers to expose important business information, consumer data, the company's innovations, and their financial situation. Subsequently, some countries, such as Germany, started to ban specific WIoT devices, such as the IoT doll which is fitted with a Bluetooth microphone that could record the voice of anyone within 25-m radius (Cavalry, 2014; Culbert, 2020; S Li et al., 2015). Software updates become critical for maintaining the security of these innovative devices after the launch of any new IoT device. However, users could not get such automatic updates, and some WIoT devices may continue to be used without such necessary updates. Furthermore, updates could negatively affect the operating system of these devices, and these changes may be far beyond the user’s expectations. Therefore, some users may decide against updating their devices, and the problem of vulnerability might escalate (Malina et al., 2016; Gessner et al., 2012; Liang et al., 2017; Chaudron et al., 2017).

2.3. Privacy concerns related to WIoT technology

The privacy problem is related to WIoT devices continuously collecting data about users. For instance, a report by Peppet (2014) showed that only 8,000 people could create 150 million data points, daily through using their devices (Peppet, 2014; Nelson, 2016). Privacy concerns represent a serious problem which could easily lead to people's dissatisfaction. The evidence comes from the WIoT device which continuously monitors the health of people for evaluation of their fitness, activity, and sleep time. Studies have shown that self-tracking users reported various dissatisfaction, such as a sense of helplessness and stress when they forget their wearable device at home or when they forget to start their activity monitoring manually while exercising (Datta et al., 2018). Also, some WIoT devices lack specific characteristics which makes them hard to be identified from other devices. For example, Google Glass wearable device may record people’s activities without people even noticing that the device is active (Datta et al., 2018). In fact, privacy concerns might be more serious than users thought. Researchers have already proven that our sensitive and confidential information collected by the WIoT devices are easy to be transfused ()

Furthermore, studies showed that the privacy concern could lead to the users being susceptible to certain outsider attacks. For instance, the sensors in smartwatches make it easy to collect the user's data on keyboards. Subsequently, users could be exposed to attacks, such as, keystroke inference ones (Liu et al., 2015). Subsequently, studies showed that users’ perceived privacy issues negatively affect their acceptance of WIoT devices (H Li et al., 2016). Although privacy issues are widely observed, some regions are more affected by the problem. This is related to their societal norms, cultures, and the application field of WIoT device. For example, consumers of self-fitness device tracker were more concerned about privacy issues than medical device users (Crager & Maiti, 2017; H Li et al., 2016). This inconsistency in opinions among people in different regions is explained by a “privacy paradox” phenomenon, which could worsen user's opinion towards WIoT instruments. Privacy paradox describes an inconsistency between users concerns and their actual behaviour (Williams et al., 2016).

2.4. Social norms

To understand the relationship between social norms and new technologies including WIoT, it is essential to know who they develop in societies. The study of Levin (2002) suggested that social norms develop in societies based on “esteem-based theory” which need a consensus about the positive or negative esteem worthiness of engaging in a particular behaviour, and also, a risk
must exist that any person who is discovered to be engaged in that behaviour, they would bear the cost of discovery, and both the existence of consensus and the risk of detection must be well known in that community. Additionally, when something is considered a social norm, the idea of changing it appears to be extremely difficult or even impossible (Levin, 2002). When dealing with new technologies, common social norms determine the reaction of the public towards it. They include confidentiality which encourages people to speak and live in their way, people’s privacy is also very essential, a sense of security and a sense of freedom which people like to enjoy in their lives. Also, users have a sense of fear, worry, and anxiety from others including strangers, relatives, governmental organisations, and insurance companies getting access to their daily information (Chang & Sanfey, 2013). Additionally, people in different regions may have different reactions to the above mentioned societal norms. For instance, people in the Middle East are more worried about relatives and families than in Western societies, while Western people prefer more freedom than their Eastern peers. So, the former group’s main concern is related to leaking their photos, and their eating habits to their relatives, while the latter group’s concern is related to leaking their daily habits, such as, their eating habits to insurance companies which may affect their insurance policies (Monther & Tawalbeh, 2020). The study by Horne et al. (2015) examined the effect of norms on user expectations of new technology. The study reported that consumers were concerned if companies sold their collected data, and if their confidentiality was not protected. Users were also concerned with the conditions under which their information was shared (Horne et al., 2015). Also, the study by Martin and Nissenbaum (2016) surveyed users for their varying concerns towards data flows. The study observed that specifying additional contextual information affected users’ perception towards sensitivity of their information. They conclude that consumers were more concerned with knowing “how the company used their information than the type and sensitivity level of their data (Martin & Nissenbaum, 2016). Additionally, the study of Marino et al. (2020), which was conducted on adolescents, showed that social norms were directly associated with poor internet communication. They concluded the importance of both peer influence and emotion regulation to control the online problem (Marino et al., 2020).

2.5. The social norms related to WIoT technology
The social use of WIoT devices could harm societies as it could weaken the relationship between people in the same societies or those from different communities. This type of social communication has some limitations as people are unable to recognise the boundaries between what is acceptable and what is forbidden. For example, if a user takes photos of strangers by simply pressing on the camera bottom without seeking their prior permission that could endanger the bonds in the community (Robinson, 2018). Also, some technical factors include, the “always online” property for many WIoT devices for them to work properly, so, the device does not communicate by the user’s “conscious” permission. Therefore, what is actually being shared, such as photos of the stranger, is usually determined by the parameters of the device, with little control from the user. For example, smart fitness tracker always collect information about the user’s habits, fitness, and their health data, such as their heart rate (Van der Zeeuw et al., 2019; Van Deursen & Mossberger, 2018). Additionally, using the WIoT socially with strangers suggests a type of social interaction that substitutes face-to-face human attachments in everyday activities. Moreover, youth spend hours on the internet for visual communication and this could negatively affect their real communication skills (Van der Zeeuw et al., 2019). Moreover, the community is expected to become over-relying on these wearable instruments. For instance, educators could find it easier to use wearable sensors than traditional ways of education. This could, in turn, harm the level of education for children and the impact of schools on children would be lost shortly (Bower & Sturman, 2015).

2.6. The effect of social norms on privacy and security concerns
Social norms could aggravate the privacy and security concerns of people and an individual’s privacy as a consequence of social norms could be a sensitive and difficult issue to deal with. Endangering the confidentiality and privacy of people could lead to unpredicted consequences (Chang & Sanfey, 2013).
Social norms have a greater impact on people’s decisions. People could either stop using the device or may stop using some important features in their device. Also, governments could restrict the whole service, for example, in 2017, Cameroon blocked Internet access for some regions for over 3 months because of privacy concerns when people in two regions spread news about people via social media which harms the community. Additionally, negative feedback from people could be devastating to the company’s figure and hence its profits (Theprivacyguru, 2014; Monther & Tawalbeh, 2020; Yamin et al., 2019). Moreover, conflicts are likely to happen between different groups of people. This is evident when some people observe “breaches to their societal norms” from others. For example, the US government has requested internet companies concerned with communication in Border States about their role in the privacy concerns of different people in a way that respects different people’s norms (Monther & Tawalbeh, 2020; Zhae et al., 2019). Studies have shown that users are particularly concerned about advertising their data, companies selling their data, type of collected data, the storage location, and the duration of storage (Yan & Holtmanns, 2008; Phelps et al., 2010).

Understanding the effect of societal norms on WIoT technology is essential for designers to develop devices that consumers are satisfied with. Also, it would guide officials and customer advocates to know and contextualise privacy violations that gain trust from users (Monther & Tawalbeh, 2020).

It is not easy to deal with such a complex problem. At a national level, while developed countries have organised discussions on the security issues of WIoT, the majority of the world’s population has little exposure to this debate. Furthermore, each nation has different social norms, and what is acceptable here is not in other places. For example, the reaction of people to autonomous cars raised an essential question that do we allow computers to decide about our lives through driving. This issue is still openly debated in America. However, this issue has led Germany to prohibit this technology. Also, every WIoT device is different, and norms will vary based on their application (Culbert, 2020).

2.7. Trust

People are intrinsically linked to IoT, and as the use of IoT applications has developed quickly, various trust concerns have emerged. When almost everything is linked to the global Internet and things, and these concerns become obvious, further exposure will disclose other security and privacy challenges, such as the integrity of data sensed and exchanged by things, confidentiality, and authenticity. Furthermore, trust is essential in IoT for enhancing user privacy, dependable data integrity, and information security. As a result, it may assist people in adopting this technology. Despite this, there is a scarcity of specific study on trust in IoT systems in the existing literature.

Trust is vital in the IoT setting since it is widespread and dependent on qualitative data (Vasilomanolakis et al., 2015). The concept of trust is used in a variety of contexts and with varied connotations. Despite the fact that trust is an important topic that has garnered a lot of attention, it is a challenging concept with no clear consensus in the scientific literature (Rose et al., 2015). In information and communication technology (ICT), trust is characterized in a variety of potential meanings and is seen as a vital aspect of digital interactions by combining confidence in computers and humans (Levitt, 2015). Security is closely related to consumers’ ability to trust their surroundings, and the Internet of Things is no different. As a result, trust in IoT can be defined as the expectation that something will be done that will not hurt the user (Leister & Schulz). Trust can also be described as the level of confidence that an entity can provide to other entities in a certain situation for certain services (Ion, M., et al.). Although trust is commonly linked with persons, it may also be related with a device or any system, stressing the importance of assessing the level of trust in a digital community.

As a result, trust in IoT is embedded at three levels: user-to-device, device-to-device, and device-to-user (Levitt, 2015). As a result, trust is separated into three categories: entity trust, machine trust, and data trust. The requirement to interact with dependable components such as actuators and sensors is
referred to as machine confidence (Daubert et al., 2015). This is an issue in the IoT ecosystem since trusting gadgets is not always possible. Furthermore, because each entity evaluates confidence in each device differently, IoT systems must cope with non-singular trust perspectives. The IoT entity trust indicates the expected behavior of users or services. Although dependable computing can be used to generate device confidence, doing so is more challenging and experimental. To create device trust, practical approaches such as dependable computing for standardized devices, as well as computational trust, must be developed (Vasilomanolakis et al., 2015). Users’ trust also demonstrates that they obtain information that they believe to be true, of a certain quality, and of a certain timeliness. The collected information can be trustworthy (useable immediately), trustworthy with alteration (useable after alteration), or unreliable (worthless). In the absence of confidence, the user must decide whether it is preferable to abstain from using specific IoT services. As a consequence, trustworthiness is one of the most crucial things to consider when developing IoT laws and regulations that allow users to exercise their rights.

2.8. Theoretical foundation and research model
Social norms are very essential to people. They affect them for various reasons, including, they want to express their sense of belonging to a certain group, they are uncertain about their best attitude in a specific situation, they expect a social reward, or because they are forced to take a certain response from others who are powerful on them. Social norms are positively linked to people’s desire to use the WIoT devices. This could be explained by the “perceived prevalence effect”. The more a person perceives that the behaviour in question is supported by a significant number of people, the greater their motivation to do that behaviour. Consequently, the behaviour of people towards a certain device affects their intention to use them. So, hypothesis 1 states that, social norms are positively linked to “perceived usefulness” and “perceived enjoyment” (Chung & Rimal, 2016; Hu et al., 2003; Lindley et al., 2019; Miller & Prentice, 2016, 2016; Yildirim & Ali-Eldin, 2019). Customers look for “perceived usefulness” and “perceived enjoyment” to accept new technologies. “Perceived usefulness” and “perceived enjoyment” are parts of the technology acceptance model (TAM) theory. Perceived usefulness’ is related to the subjective thought which determines that using a specific technology would enhance someone’s achievement. Perceived enjoyment is related to the improvement of the level of enjoyment from such technology (Qingxiong & Liu, 2006).

Applying the “perceived usefulness” and “perceived enjoyment” in the WIoT technology, they are likely to encourage customers for their continuance intention. Thus, hypothesis 2 states that “perceived usefulness” and “perceived enjoyment” are positively linked to people’s desire to use the WIoT devices. Subsequently, the author states that (hypothesis 3), social norms are positively linked to people’s desire to use the WIoT devices (Talukder et al., 2019; Van der Zeeuw et al., 2019). On the other hand, privacy and security concerns harm people’s intention to use the WIoT technology and “perceived usefulness” and “perceived enjoyment”. This is related to the “trust theory”. Trust refers to the willingness of consumers to be vulnerable to some actions based on their belief that others respect their ethical and societal norms. On the other hand, mistrust could lead to people distrust on others, shying away from contributing with the public, and becoming compliant to take part in the community when others do not respect their social norms. Privacy and security concerns could lead to different behaviour-related aspects, including individuals avoiding the use of these devices and hence affect their “perceived usefulness”, and “perceived enjoyment”. Therefore, societal norms, privacy, trust, and security issues related to the WIoT devices could affect behavioural intention (Chau et al., 2019; Chung & Rimal, 2016; Miller & Prentice, 2016, 2016).

2.9. Research model
This study investigates the effects of security, societal norms, trust, and privacy of users’ on their behavioural intention. This study postulates that users’ behaviour is affected by four components which are security, their norms, trust, and privacy as shown in Figure 1.
3. Methodology

To understand the relationship between security, social norms, trust, and privacy concerns of WIoT devices, the current study applies a systematic research method that focuses on data gathering and analysis.

The current work consists of a review of the literature to understand the impact of security, social norms, trust, and privacy of WIoT on behavioural intention. The authors believe that a review of the literature is the starting point for having the first set of data. A literature search was performed between September and November 2020 and searched for publications written in English only. Publications included those published between 2010 and 2020, research concerned with the relationship between social norms and privacy, and security concerns of WIoT, published in peer-reviewed journals and relevant to the research questions. The authors searched for words including social norms, WIoT technology, privacy, and security of WIoT. The literature review was followed by a survey. The authors developed a survey and collected responses from customers of wearable technology in Saudi Arabia. The authors sent an invitation to the participants via e-mail, Facebook, and Instagram. Data collection took place from 1 December 2020 to 31 March 2021. The authors used a survey in the English language to test the hypotheses in the theoretical model and to collect data from the sample. Four constructs with 19 questions were used. Constructs include general items (four questions), security (five questions) social norms (five questions), trust (five questions), privacy (five questions), and behavioural intention (five questions). The survey used a combination of open-ended questions, such as have you ever used a wearable technology product? Have you ever been a victim of an attack through your wearable device? What is your main concern about the security of your device? and closed-end questions, such as do not have control of their collected data. Other questions were added to test the behaviour of users with the privacy and security of their wearables and how manufacturers should improve these security and privacy issues. The items were measured on 5-point scale (1 completely disagree, 5 completely agreed). Users who lack experience with wearable devices were excluded from the study (Riahi et al., 2013; Whitmore et al., 2015; Da Xu et al., 2014).
4. Results and discussion
Statistical analysis was carried out by SPSS 26.0. Continuous data were presented as mean, median, and range. P-value was significant if $\leq 0.05$. The response of the sample to the included survey was presented in percentage and range. From Table 1, it can be concluded that the demographic distribution of respondents is balanced and representative. The incomes of most are in the range of 5000 to 15,000, which is in perfect agreement with the comparison of the known national economy. The majority of respondents (145) own education, which has the highest number of college and above education. Table 2 signifies the construct reliability in terms of convergent validity. Since the value is higher than 0.70 hence the constructs are reliable enough of further consideration for analysis.

Before hypothesis testing, the quality of the measurement model has been evaluated as a valid and reliable. The validity of the mentioned model, including the validity of the content and the validity of the composition, has been considered first. Content validity illustrates measurements indication and their composition. This study concept model possesses satisfactory content validity, as all items were adopted in a previously published study. If the composition is valid, the convergence validity and the judgment validity are verified in. The degree to which the measured configuration does not reflect other configurations is called the discriminant validity, with the accuracy of the measured configuration as convergence valid (Gao et al., 2015, p. 1712). The proposed conceptual model for this study is Gao et al. (2015). The WTAH framework has been integrated. Hence, in the empirical study, all loads reflecting convergence validity were confirmed as construct discrimination validity. Therefore, in the study the conceptual model results to satisfactory data in the configuration validity. The internal consistency and reliability were taken for confirming the reliability of the measurement model, which is determined by Cronbach’s alpha value. This measures the degree to which participants in this study consistently responded to different items measures each variable, especially when using composite measures. Checks the reliability of internal consistency Tests for consistency in which multiple items measure the same configuration. Table 3 presents all Cronbach’s alpha value of in this study.

4.1. Cronbach’s Alpha values
The value of Cronbach’s alpha must be higher than 0.7.

4.2. Measuring structural model and testing hypothesis
Based on the results of the Cronbach’s alpha value, it can be concluded that the stability of all variables was reached. The arithmetic mean for each component is then calculated. The calculated arithmetic mean is the final value for all independent and dependent variables (Trust, Security, Social Norms, Privacy, and BI) and is added to the SPSS data matrix.

4.3. Regression analysis
In this section, we test the hypothesis by means of SPSS multivariate regression analysis to test whether the relationship between several dependent as well as independent variables are in linear sequence. A positive linear relationship defines increase in the independent variable will lead to an increase in the dependent variable (p. 130). Hence, the conceptual model illustrates that the independent variables were based on performance expectation, pleasure motive, effort predictive function concordance, social impact, perceived privacy risk, and health consciousness. The outcome (dependent variable): behavioral intent to employ wear. The descriptive statistical results verify that all dependent and independent variables are normally distributed. This satisfies the prerequisites for linear regression.

The coefficient of determination $R^2$ modified in Table 3 of the model summary shows a value of 0.615 (the proportion of variance described), which indicates that the conceptual model better predicts the actual data points (goodness of fit). The following scatterplot (Figure 2) shows that all the behavioral intentions employing wearable devices are linearly correlated.
Some researchers mentioned that standard p-values are insufficient precise indicator for statistical significance, especially if the values are provided only in groups (, p. 439). In the present study, the traditional significance level is still shown by asterisks beside parameter: \* = p<0.05 (non-significant). However, some literature illustrates that with p-value between 0.05 and 0.1; hence, there is still a chance of weak evidence that the null-hypothesis is not significant (Massey University, 2019).

In Table 4, considering the significance level of the “standard coefficient”, the statistical results support hypotheses are H1 and H2 of the factors that influence consumers’ IoT adoption, Social

| Table 1. Sample characteristics (n = 200) |
|----------------------------------------|
| Variable                  | Category | Frequency | Percent (%) |
| Gender                    | Male     | 87        | 43.5        |
|                           | Female   | 113       | 56.5        |
|                           | 18–25    | 7         | 3.5         |
|                           | 26–40    | 73        | 36.5        |
|                           | 41–55    | 55        | 27.5        |
| Age                       | 56–70    | 39        | 19.5        |
|                           | >70      | 26        | 13          |
| Missing Value             |          |           | 0           |
| Monthly Income in SAR     | <5000    | 15        | 7.5         |
|                           | 5001–15,000 | 103   | 51.5        |
|                           | 15,001–30,000 | 35 | 17.5        |
|                           | 30,001–50,000 | 18 | 9           |
|                           | >50,001  | 7         | 3.5         |
|                           | No information | 22 | 11         |
| Missing Value             |          |           | 0           |
| Highest Education         | high school | 22   | 11         |
|                           | College  | 29        | 14.5        |
|                           | University | 145  | 72.5        |
|                           | No information | 4  | 2          |
| Missing Value             |          |           | 0           |

| Table 2. Reliability test (n = 200) |
|-----------------------------------|
| Variable Items (Construct)        |
| SS1, SS2, SS3                     | Security | 0.861 |
| SI1, SI2, SI3                     | Social Norm | 0.914 |
| TR1, TR2, TR3, TR4                | Trust    | 0.888 |
| PPR1, PPR2, PPR3,                 | Privacy  | 0.867 |
| BI1, BI2, BI3                     | Behavioral intention | 0.908 |

| Table 3. Multivariate regression model summary |
|------------------------------------------------|
| Model | R  | R² | Adjusted R² | Std. Error of the Estimate |
|-------|----|----|-------------|----------------------------|
| 1     | .791 | .625 | .614 | .673595 |
Norms (β = 0.474; p < 0.000) and Security (β = .104; p < 0.030) are significant determinants. However, the impact of effort expectations is so weak that it can be almost ignored. Therefore, hypotheses H3, and H4 are discarded in this study. Nevertheless, there can be a difference between their respondents, which is analyzed for an additional through the accommodative effects of national variables.

The test results are summarized in Table 5. The “Effect” is the conditional effect (coefficient) of a predictor focusing on the value of the moderator. LLCI represents the lower bound of the confidence interval and ULCI represents the upper bound of the confidence interval.

Hence, based on Table 5, the conceptual model is significant with the predictors: trust the model, sig. value = 0.0001 (weak) and perceived privacy risk of the model, sig. value = 0.0041. The involvement of variables, the influence of trust for the user intention of Saudi respondents (β = 0.6068; p < 0.000) is positive and bita coffecient is strong; the influence of trust for the user intention, however, remains insignificant. Therefore, trust would not likely be predictor factors for intention to adopt WIoT. Similarly, with the involvement of variables, the influence factors of perceived privacy risk on the user intention remain insignificant. Thus, perceived privacy risk would not be a predictor, which influence the intention of Saudi users to adopt WIoT devices. Therefore, the influential factors, Social security, and social Norms affect behavior intention positively that support the hypotheses H1 and H2, respectively. Functional congruence, trust, and perceived privacy risk do not affect BI significantly; hence, H3 and H4 are discarded, respectively.
This research provides multiple implications to the existing literature on WIoT technology. The current work identified and examined the relationship between factors and their and their influence on wearable devices. The authors believe that despite the enormous benefits the users are getting from the WIoT technology in terms of improving interactions, however, their privacy and security challenges need to be addressed and dealt with by the manufacturers while designing the WIoT and this must be communicated to the user to reduce dissonance. Additionally, the study stated that the social norms of people negatively affect the privacy and security challenges of the WIoT and could compromise it. Furthermore, there are suggested measures that could help to improve the security and privacy of the WIoT devices.

The relationship between social norms and the WIoT technology has not been well studied in earlier research, and to the knowledge of the authors, the current work is one of the earliest studies which looked at this cause–effect relation. Also, the current study used strict predefined criteria for literature review to avoid bias and to improve the quality of the current work. Social norms have a great impact on people’s decisions. For example, it determines how we deal with strangers, when and whom to marry and what career to choose. (Chang & Sanfey, 2013)

This study provides important suggestions for manufacturers which could improve the technology in a way that respects societal norms and improve the privacy and security of people. Solutions include strict legislation, consents, companies to seek people's opinion in advance, GDPR principles, avoid indefinite storage, frequent updates, and user's education.

5. Conclusion
The main dependent variable or output in this study is the behavioural intention of an individual to use IoT wearable devices; hence, the aim of this study was to identify which factors can predict this dependent variable.

The current study confirms that perceived privacy risks have a greater impact on the intention to adopt wearable devices. It has also been drawn from studies that validate health awareness is a major predicting factor for the intention to adopt wearable devices. “Security and social impacts have a significant impact on the intent to adopt wearables”, is not supported in arbitration analyses like the numerical “model signature”. On the contrary, trust may not be a predictor that influences the intent to adopt a wearable device. The study also illustrates that security and social impacts do not support intervention analysis on the intention to adopt wearable devices. The study suggests the manufactures to address in establishing relationship and should be concerned towards customers' privacy and social norms that are mentioned in detail in the recommendation section. Advancement in technology in fulfilling privacy and legislation has to be top-notch and penalization of those required in regard to breach of privacy. To maximize the probability and acceptance among consumers, protocol for WIoT devices and consent need to be communicated to the user. Awareness among the use of WIoT needs special attention. Although the WIoT presents an opportunity to revolutionize our lives, there remain some potential challenges linked with that technology. There are several opportunities for further research. The population of this study showed many similarities in gender, age, education,
and nationality. More specifically, the participants were mainly educated males from Saudi Arabia. It is therefore possible that a study with another sample will present different findings, for example, when looking at different cultures. As this study was conducted within a specific niche, further studies should be conducted at different organizations before one can generalize the results obtained in this paper.

5.1. Recommendation

5.1.1. Customer opinion in advance
Device manufacturers should survey societal norms in advance. For example, if a company creates smart TV or a headphone product in a certain region, communicate with customers in advance to ask about their opinion. Manufacturers could know that gaining certain data, such as house occupancy and consumer eating habits, is unacceptable in that community. Then, manufacturers could create specific protocols that suit them in that particular region. Additionally, customers may ask for some minor changes to accept the product. For example, for the IoT toy “spying” on children, studies showed that consumers were annoyed that the instrument indefinitely stored data of their youngsters. Therefore, if such data are automatically deleted by the company each day, or if adults get access to manually delete their child information, this would increase user satisfaction.

5.1.2. User consent is important
Studies have shown that consumers tend to accept information transfer with their consent only, if they give their consent to their information to be collected, stored, and shared. However, there are lot of challenges because service providers have to tell customers exactly what data are collected and what they are to be used for, which is practically difficult for WiIoT technology. (ICO, 2017; Peppet, 2014)

5.1.3. Information sharing should avoid outdoors flows
It could be acceptable for people, according to their social norms, to have data flows inside rather than outside their houses. For example, if a wearable smartphone sends its user’s place to a nearby indoor device, users may feel that their data flow is acceptable given user privacy norms are maintained. However, if the same instrument sends such information to the cloud or to other instruments outside the home, this type of information flow would not be acceptable. Companies should prevent devices from sending potentially sensitive information about users. Measures could include the obfuscation technique to avoid violating information flow from certain devices, especially security cameras, refrigerators, and door locks (Matyszczek, 2015).

5.1.4. Device communication should directly support primary functionality
Data flow could be acceptable if it is closely related to the primary device function. For example, for a fitness tracker to work, it would need data about the heart rate and exercise routine of its user. Such a data leak is likely to be acceptable among users than a refrigerator sending data about the position of their users (Nissenbaum, 2010).

5.1.5. Legislation with Enforcement
A law that ensures the privacy of users will certainly improve the problem. Europe’s General Data Protection Regulation (GDPR) is a good example. The GDPR requires internal evaluation of the company’s practice and manufacturers which fail to comply face sanction, and manufacturers should inform the government about any data breaches immediately. Additionally, companies that fail to meet their requirements could be fined up to 4% of their annual revenue (Scott 2014, Jones & Meurer, 2016). Also, companies are required to conduct mandatory privacy impact assessment to evaluate the risks of sharing and using identifiable information about people. They should only collect consumer’s data for specific reasons and are not allowed to use user’s data in ways below their expectations. In addition, users should be offered the option to update the device privacy settings during the collection process (Slomovic, 2015).
5.1.6. Devices with Greater User’s Control

Users should be offered greater control of their WIoT devices; manufacturers could design “Do Not Collect” permission so that users could reduce or turn off the feature of information collection. Also, companies could alert the user that they start collecting data if a customer uses a “wake word” activities, such as when users say “Alexa” in Amazon devices. Also, manufacturers should design new WIoT devices to manage people’s identity as a priority. They need to manage how people are authenticated to log in, and whether people could log in with pseudonyms or anonymous guest access (Suhluli, 2021).

6. Limitation and future research

The current study has some limitations. Firstly, this research was carried out in Saudi Arabia this limits its implication on a global level. Further research is required to compare countries with different ethnic groups and between different regions, such as urban and rural, in the same country. For example, this could include countries in North America, and the Middle East. Secondly, the sample size, although it was homogenous, was not big enough to represent the whole society, future research should include a bigger sample size to better understand consumers’ opinion. Furthermore, this trial focused on the social norm’s impact on the privacy and security concerns of consumers and it ignored other important factors which also determine people’s opinion, such as price and durability. Thus, future research is advised to include other factors to explain consumers’ adoption intentions. Besides, future research could examine the perspectives of different cultures, corporate, and societal, and involve a greater number of respondents. Future research could also perform multi-group analyses to examine whether the control variables have effects on the path of the model.

Funding

The authors received no direct funding for this research.

Author details

Syed Salem Ali Suhluli 1
E-mail: ssuhluli@gmail.com
Syed Md. Faisal Ali Khan 1
ORCID ID: http://orcid.org/0000-0003-2335-2052

1 Department of MIS, College of Business Administration, Jazan University, Jazan, Saudi Arabia.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Citation information

Cite this article as: Determinants of user acceptance of wearable IoT devices, Salem Ali Suhluli & Syed Md. Faisal Ali Khan, Cogent Engineering (2022), 9: 2087456.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). A survey on enabling technologies, protocols, and applications of the internet. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Ali, D. H. (2015). A social Internet of things application architecture: Applying semantic web technologies for achieving interoperability and automation between the cyber, physical and social worlds. [Ph.D. thesis]. National Institute of Telecommunications.

Bower, M., & Sturman, D. (2015). What are the educational affordances of wearable technologies? Computers & Education, 88, 343–353. https://doi.org/10.1016/j.compedu.2015.07.013

Canhoto, A. I., & Arp, S. (2017). Exploring the factors that support adoption and sustained use of health and fitness wearables. Journal of Marketing Management, 33(1–2), 32–60. https://doi.org/10.1080/0267257X.2016.1234505

Cavalry. (2014). Five star automotive cyber safety framework. I Am The Cavalry. August 2014. Accessed July 4. https://iamthecavalry.org/5star

Chakraborty, P., Neogi, B., & Das, A. (2020). Knowledge Based database of arm-muscle and activity characterization during load pull exercise using Diagnostic Electromyography (D-EMG) Signal. Cogent Engineering, 7(1), 1849946. Zhongmin Jin (Reviewing editor). https://doi.org/10.1080/23311916.2020.1849946

Chang, L. J., & Sanfey, A. G. (2013). Great expectations: Neural computations underlying the use of social norms in decision making. Social, Cognitive, & Affective Neuroscience, 8(3), 277–284. https://doi.org/10.1093/scan/nsr094

Chau, K. Y., Cheung, M. L., Lam, H. S., Tso, K. H., Flint, S. W., Broom, D. R., Tse, G., & Li, K. Y. (2019). Smart technology for healthcare: Exploring the antecedents of adoption intention of healthcare wearable technology in Hong Kong. Health Psychology Research, 7(1), in press. https://doi.org/10.4081/hpr.2019.8099

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer’s dilemma. Information Technology Management, 6(2), 181–202. https://doi.org/10.1007/s10799-005-5879-y

Chen, J., & Dibb, S. (2010). Consumer trust in the online retail context: Exploring the antecedents and consequences. Psychology & Marketing, 27(4), 323–346. https://doi.org/10.1002/mar.20334

Chung, A., & Rimai, R. N. (2016). Social norms: A review. Review of Communication Research, 2016(4), 1–28. https://doi.org/10.12840/2255-4165.2016.04.01.008

Cislaghi, B., & Heise, L. (2020). Gender norms and social norms: Differences, similarities and why they matter in prevention science. Sociology of Health & Illness, 42(2), 407–422. 2020 0141-9889. https://doi.org/10.1111/1467-9566.13008.
Crago, K., & Malti, A. (2017). Information leakage through mobile motion sensors: User awareness and concerns. Proceedings of the European Workshop on Usable Security (EuroUSEC). https://doi.org/10.14722/eurousec.2017.23013

Culbert, D. (2020). Personal data breaches and securing IoT devices. betanews.com/2019/08/13/securing-iot-devices.

Da Xu, L., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243. https://doi.org/10.1109/TII.2014.2300753

Datto, P., Namin, A. S., & Chatterjee, M. (2018). A survey of privacy concerns in wearable devices. Conference: 2018 IEEE International Conference on Big Data (Big Data). https://doi.org/10.1109/BigData.2018.8622110

Daubert, J., Wiesmoer, A., & Kikiras, P. (2015). A view on privacy & trust in IoT. In: 2015 IEEE International Conference on Communication Workshop (ICCW). IEEE.

Eriçen, S. D T Pham (Reviewing editor). (2022). IoT-Based Real-Time updating multi-layered learning system. applied for a special care context during COVID-19. Cognet Engineering, 9(1), 2044588. https://doi.org/10.1080/21331916.2022.2044588.

Flaherty, J. L. (2014). Digital diagnosis: Privacy and the regulation of mobile phone health applications. American Journal of Law & Medicine, 40(4), 416-441 doi:10.1177/0301105209107401 [PubMed] [Google Scholar].

Gessner, D., Oliveira, A., Segura, A. S., & Serbanati, A. (2012, June 25–27). Trustworthy infrastructure services for a secure and privacy-respecting internet of things. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 998–1003).

Granjo, J., Monteiro, E., & da Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communication Surveys & Tutorials, 17(3), 1294–1312. third quarter, 2015. https://doi.org/10.1109/COMST.2015.2388550.

Greenberg, G. D., Miller, J. A., Mohr, L. B., & Vladeck, B. C. (1977). Developing public policy theory: Perspectives from empirical research. The American Political Science Review, 71(4), 1532–1543. https://doi.org/10.2307/1961494.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Habibipour, A., Padyab, A., & Stolhrbst, A. (2019). Social, ethical and ecological issues in wearable technologies. Twenty-fifth Americas Conference on Information Systems, Cancun (pp. 2019).

Hamblen, M. (2015). As smartwatches gain traction, personal data privacy worries mount: Companies could use wearables to track employees’ fitness, or even their whereabouts, in computerworld Computer World.

Harne, C., Darras, B., Bean, E., Srivastava, A., & Frickel, S. (2015). Privacy, technology, and norms: The case of smart meters. Social Science Research, 51, 64–76. https://doi.org/10.1016/j.ssrresearch.2014.12.003

Hu, P. J. H., Clark, T. H. K., & Ma, W. W. (2003). Examining technology acceptance by school teachers: A longitudinal study. Information Management, 41(2), 227–241. https://doi.org/10.1016/S0378-7206(03)00050-8

IBM Watson Foundations. (2015). Maximize Insight, Ensure Trust and Improve IT Economics – United States.

Accessed 2017, July 4. https://www.ibm.com/big-data/us/en/big-data-and-analytics/sft-economics.html

ICO. (2017). GDPR consent guidance for consultation. Accessed 2017, July 4. https://ico.org.uk/media/about-the-ico/consultations/201555/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Jones, M. L., & Meurer, K. (2016, May 13-14). Can (and Should) hello barbie keep a secret? 2016 IEEE International Symposium on Ethics in Engineering, Science and Technology, Vancouver, BC. https://papers.rsna.org/si3/papers.cfm?abstract_id=2768507 IEEE.

Kumar, N., Madhuri, J., & Channe Gowda, M. (2017). Review on security and privacy concerns in internet of things. In 2017 International Conference on IoT and Application (ICIOT) (pp. 1–5). https://doi.org/10.1109/ICIOT.2017.8073640

Lee, Y., Yang, W., & Kwon, T. (2018). Data transmission: Focusing wearable devices and its implication on security for internet of things. IEEE Access, 6, 48994–49006. https://doi.org/10.1109/ACCESS.2018.2859046.

Levin, D. B. (2002). Building social norms on the internet. Yale Journal of Law & Technology, 2, 99 https://open.yislaw.yale.edu/bitstream/handle/20.500.13051/783/Levin_Tech%20Report%204.pdf.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals’ adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. International Journal of Medical Informatics, 88, 8–17. https://doi.org/10.1016/j.ijmedinf.2015.12.010.

Liang, G., Weller, S. R., Juhanuo, Z., Fengli, L., & Zhao, Y. D. (2017). The 2015 Ukraine Blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems, 32(4), 3317–3318. https://doi.org/10.1109/TPWRS.2016.2631891.

Lindley, J., Couton, P., & Altera, H. (2019). Networking with ghosts in the machine. Paper presented at the Running with Scissors, 13th EAD Conference (pp. 1–13). Dundee: Taylor & Francis Group.

Liu, X., Zhou, Z., Diao, W., Li, Z., Zhang, K. (2015). When good becomes evil: Keystroke inference with smartwatch. In: 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1273–1285). ACM. https://doi.org/10.1145/2810103.2813668.

Malina, L., Hajny, J., Fujidiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. Computer Networks, 102, 83–95. https://doi.org/10.1016/j.comnet.2016.03.011

Marino, C., Gini, G., Angelini, F., Vieno, A., & Spada, M. M. (2020). Social norms and e-motions in problematic social media use among adolescents. Addictive Behaviors Reports, 11(June), 100250. https://doi.org/10.1016/j.abrep.2020.100250.

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. Columbia Science and Technology Law Review, 18 1, 176 https://doi.org/10.7916/stlr.v181.4015.

Martin, K., Shilton, K., & Smith, J. (2019). Business and the ethical implications of technology: Introduction to the symposium. Journal of Business Ethics, 160(2), 307–317. https://doi.org/10.1007/s10551-019-04213-9
Morchon, and Klaus Wehrle. 2014. https://doi.org/10.1109/JIOT.2014.2306328.
Zhao, E. Y., Thatcher, S. M., & Jehn, K. A. (2019). Instigating, engaging in, and managing group conflict: a review of the literature addressing the critical role of the leader in group conflict. Academy of Management Annals Vol 13(1), 1 https://doi.org/10.5465/annals.2016.0153.