THE IMPACT OF MANIPULATING IOT WEARABLE CONTROLS ON USERS PRIVACY CONCERNS

Salem Suhluli, Jazan University

ABSTRACT

IoT wearable devices have inferences for fitness and health, whilst, fitness wearable can encourage healthy behaviour and enhance an individual's entire health along with quality of life. Although fitness wearables have numerous benefits, privacy concerns associated with data gathered stay as a main barrier to implementation of fitness wearables. The aim of the research is to investigate into the impact of manipulating IOT wearable devices' control on the privacy concerns. The objective of the research is to explore the possibilities of eliminating or reducing the privacy concerns in the health care sector, since it is among the sectors commonly facing privacy concerns in both developed and developing countries. The insight and feedback of end-users carry equal importance for creators for developing optimal devices, and to empirically identify and test the individual attitude. This study emphasises on interpretivism philosophy, in support of deductive approach which is affiliated with the particular understanding of and interference in actuality. The researcher has taken a deductive approach, which has obliged with social theory and then testing its implementation with data. The quantitative method has been chosen by the researcher to collect the data for the survey. There were 250 respondents who participated in the survey. In addition, after collecting the data ANOVA analysis was performed to relate the demographics of the respondents of the groups.

Keywords: IOT wearable; Privacy concerns; Manipulation; Stakeholder and authentication process; Data classification; Password protection; Access controlling; Storage location; Connectivity and compliance.

INTRODUCTION

The wearable device is recognised as the new electronic technology associated with sensor and accessory structures, has presented its importance in numerous fields (Thierer, 2015). Whilst, wearable technologies are regarded as networked devices, which help in tracking activities, collecting data and customising experience associated with users' requirements and needs. Moreover, these technologies are known as the subset of IoT that entails networked "smart devices" equipped with microchips, wireless connections, and sensors. IoT wearable devices have inferences for fitness and health; whilst, fitness wearable can encourage healthy behaviour and enhance an individual's entire health along with quality of life (Li et al., 2016). Although fitness wearables have numerous benefits, privacy concerns associated with data gathered stay as a main barrier to implementation of fitness wearables. With the upsurge extent of "Internet of Things (IoT)" services, such as sensor-based IS services enabled through the identification of technologies, for examples, radiofrequency, global satellite communication or barcode, experience new privacy concerns within their professional and personal lives (Kowatsch & Maass, 2012).

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

Subsequently, wearable technologies are amongst the fastest-growing section of IoT and committed to having extensive social impacts in the coming years. The development of wearable device offers more prospects for back-end workers (start-ups and App developers) along with big data analytics enterprises (Li et al., 2016).

Nonetheless, it has been identified that health information within real-time has extensively implemented in the healthcare domain. Currently, fitness and clinical wearable instruments are recognised as the two major types of healthcare wearable (Parashar, 2016). Through approving and implementing an appropriate fitness wearable device, i.e., Jawbone UP and Fit bit flex, operators could manage their health concerns, for example, calories burned, heartbeat, distance covered in real-time and sleeping routine (Thierer, 2015).

Aims and Objectives

The aim of the research elaborates the purpose of the cause for researching as it explains in one sentence what the researcher expects to attain whilst concluding the project. The aim of this study is to investigate into the impact of manipulating IOT wearable devices' control to reduce users' privacy concerns. The objective of the research is to identify the ways of reducing privacy concerns using the privacy controls of wearable devices.

Significance

Internet of Things provide massive benefits; whilst, there are some challenges as well. Thus, the purpose of this study is to demonstrate about the importance of IoT wearables that could be manipulated to see whether privacy controls are reducing privacy concerns or not. This can contribute in the healthcare sector and the companies operating within it to become more confident about the data being secured and protected, which in turn can influence in the reliance on more IoT wearable devices for better and improved quality of care.

Research Question

It has been identified that a research question is associated with the core of systematic exploration and the reason behind stating the research question is to demonstrate the reason for conducting the research effectively. Whilst, the question of the research is:

What is the impact of manipulating IoT wearable devices' control on the privacy concerns?

LITERATURE REVIEW

A study demonstrated that the Internet of Things (IoT) service offers new privacy and security issues in daily life especially for healthcare domain such as password protection and detection (Kowatsch & Maass, 2012; Parashar, 2016). Whilst, no empirical device has emerged for IoT services, which determines privacy aspects that forecast usage individual's keenness in order to deliver personal data (Kowatsch & Maass, 2012). Nonetheless, the influence of this study is to focus on the gaps of the prior research, yet the results demonstrated that objectives for using IoT facilities are impacted through numerous aspects. In the study of "Security and Privacy of Wearable Internet of Medical Things" considering the perspective of stakeholders explained that wearable technology has presented the perspective of enhancing healthcare effectiveness and decreasing cost of healthcare (Kowatsch & Maass, 2012; Li et al., 2016). Nevertheless, different

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

by pioneering researches affiliated with healthcare wearable devices through technical viewpoint (Li et al., 2016).

It can be analysed that various fundamental drivers of the Internet and Information Age uprising – an enormous upsurge in processing power, explosion of storage capacity, pervasive wireless network and its abilities, stable diminishment of computing and cameras, digitisation of all information, immense datasets (big data) are recognised as the starting for having an intense impact beyond the restrictions of cyberspace (Thierer, 2015). Whilst, on the contrary, it has been demonstrated that there are various applications, such as Facebook Places, Groupon tracking, Google Places and Foursquare, which enable to track the location of the service users in order to offer value-added experience through basic agreement: provide surety for the privacy of data and getting important information (Samaila et al., 2018). Considering the above-mentioned examples, it is quite clear and obvious for the users to be aware of the tracking location-based information. Whilst, not every time it is evident that type of data is pursued at which time. For example, when these services are operating or sometimes users forget to dismiss them (Li et al., 2016; Parashar, 2016; Thierer, 2014). Nevertheless, serious concerns can occur, such as when the information is associated with Facebook or Twitter and then utilised to commit wrongdoings, i.e. breaking into an empty house (Parashar, 2016; Thierer, A.D., 2014).

For this invention, various innovative organisations, i.e., Apple and Google are striving to study more about medical wearable devices (Putta et al., 2020; Zhu, Gai, & Li, 2019). Hence, users might only monitor their fitness parameters, yet they can also attain customised medical recommendations, additionally receiving their physical information, for instance, gene expression, blood pressure, and oxygen level (Tawalbeh et al., 2020). The recent study was published through P&S Market research, which elaborates about the international healthcare wearable device (which involves medical and fitness wearable devices) in 2014 market was project for 155 million dollars, and expected to reach 1635 million dollars in 2020 associated with 45 per cent growth rate from 2015 to 2020 (Thierer, 2014). Currently, the wearable healthcare devices' market has a market worth of 18.4 billion dollars and is expected to rise to 46.6 billion dollars by the end of 2025 (Markets & Markets, 2020). Therefore, wearable devices might have enormous potential growth in upcoming years and it has been identified that providing different and innovative facilities to the service users could help them to understand the technology effectively. It will eventually result in saving cost and time of the users (Bhatt, Patwa & Sandhu, 2017; Samaila et al., 2018; Thierer, 2015).

Wearable Technology

Currently there are many extant types of research regarding healthcare wearable devices, which have emphasised on a technical standpoint. However, they are affiliated with making constant efforts to discovering new and innovative technology, which could be implemented within the healthcare sector (Thierer, 2015). Though the insight and feedback of end-users carry equal importance for creators for developing optimal devices, the study on empirically identifying individual's attitude, such as the implication of adoption for healthcare wearable devices is scarce (Parashar, 2016; Zhu, Gai, & Li, 2019). Through conducting the research of preceding "Health Information Technology (HIT)" adoption study, the researcher has initiated that many extant affiliated studies examine an individual's adoption for HIT through healthcare and technical behaviour viewpoint (Parashar, 2016). Moreover, the researcher perceived that

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

examining the behaviour of users through healthcare domain is much easier as compared with other domains (Poongodi et al., 2020).

Undoubtedly, privacy concerns have an analytical role in examining individual's aim to adopt and implement HIT because of the higher and better understanding of healthcare data, merely few of the studies have regarded the aspects associated with the perception of security as independent variables and without any additional exploration of privacy perception development (Bhatt, Patwa, & Sandhu, 2017). It has been determined that there are several issues, for instance, spoofing attacks and jamming and some unlawful access that have cooperated the reliability of users' information. In order to protect IoT devices, there are some reasonable and practical outcomes, which could assist an individual in implementing numerous security measures (Arias et al., 2015; Kowatsch & Maass, 2012). Nonetheless, several privacy challenges have appeared currently, and they might pierce IoT Technologies with their assimilated network. Yet, it has been identified that it is quite difficult to monitor the protection of IoT devices within firms and businesses (Dai et al., 2017; Zhu, Gai, & Li, 2019). Whilst, firms should arrange managing and tracking techniques for the IoT devices, which can discover any kind of issues associated with security and strive to alleviate the threat of being penetrated. The information provided that the users regardless of the domain should be kept confidential and ensuring that the data will not be mishandled in future. Moreover, this credibility by the firms could assure the long-term relationship of the users and stakeholders such as service users, service providers, etc. (Parashar, 2016; Thierer, 2014; Yildirim & Ali-Eldin, 2019).

Privacy Challenges

It has been analysed that cybersecurity and privacy challenges are classified as the fundamental issues of the researches, as these two concerns are demonstrating a substantial predicament for various businesses and firms (Bhatt, Patwa, & Sandhu, 2017), whilst, it has been elaborated that the liabilities and challenges of IoT technologies are associated with predominant high-profit of cybersecurity (Thierer, 2014). As these liabilities are regarded as the interconnectivity of networks in the IoT carries with availability through unidentified Internet necessitating original security outcomes. Since, all the concerns, which are identified, none of them have a more momentous impact on the implication of the Internet of Things, for example, privacy (Alharbi & Almagwashi, 2019). Nonetheless, it is unfortunate for the users who do not usually need the acknowledgement for security influences unless the time when any kind of breach has occurred, creating huge indemnities, for example, losing important information (Amyx, 2017; Bhatt, Patwa, & Sandhu, 2017). By analysing these theories, it was examined that many users are not that much friendly or comfortable with the technology just because of the security and privacy concerns, which makes them outdated and with minor insight of the current trends (Tawalbeh, et al., 2020). Thus, this is recognised as the major challenge of IoT that needs to be addressed and resolved effectively.

However, there are numerous challenges, such as spoofing and jamming attacks along with other unofficial access that have conceded the reliability of the user's information, while, some privacy challenges have developed in the current time, and they might penetrate IoT wearables with their integrated system (Meng, et al., 2018). Considering several businesses and organisations, it is quite difficult to manage the privacy of the employees and other stakeholders, such as managers, customers, etc. For instance, the unconscious use, not preferring to change passwords, and not updating devices have extensively upsurge cyber security challenges and

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

access to malevolent implementations to the Internet of Things systems' sensitive data, this will eventually result in unfortunate privacy practices upsurge the possibilities of breaching of data or some other threats (Makhdoom et al., 2018; Siby, Maiti, & Tippenhauer, 2017). However, security professionals recognise IoT as the vulnerable point for cyber-attacks because of poor privacy practices and procedures. Although various privacy mechanisms were emerged for protecting IoT devices from cyber-attacks, therefore, privacy and security guidelines were not properly documented (Aldwairi & Tawalbeh, 2020). In this regard, corporate workplaces and personal devices usually challenge privacy concerns because of high-profile attacks, which can be resolved if device manufacturers and security specialists assess the cyber threat appropriately, they might emerge an effective protecting tool to avoid or neutralise cyber threats (Menget al., 2018; Siby, Maiti, & Tippenhauer, 2017). The theory of privacy calculus is associated with investigating the implication of wearable devices (Banerjee, Hemphill, & Longstreet, 2018). Whilst, privacy calculus was initiated by Laufer and Wolfe, they declared that prior to revealing sensitive and important information; people frequently relate social benefits with underlying destructive concerns, which will be brought up by disclosure. Subsequently, the model was then implemented in "Information Systems (IS)" domain, in which privacy calculus theory has been extensively embraced to elaborate customer's objective to reveal personal and sensitive data in numerous contexts, such as social commerce, location-based service and electronic commerce (Parashar, 2016; Thierer, 2015). Nonetheless, considering the background of electronic health, merely some studies have engaged privacy calculus theory in order to observe "individual's health information sharing behaviours" along with their implication with "personal health records (PHR)" (Parashar, 2016). Whilst, in accordance with the wearable devices, they are not only revealing distinguishing advantage on enhancing the effectiveness of healthcare, yet also generating greater extent of privacy challenges, decisions taken by individuals for adopting privacy calculus so that users might experience the trade-off amongst apparent advantage and privacy risk (Tawalbeh et al., 2020).

Research Model

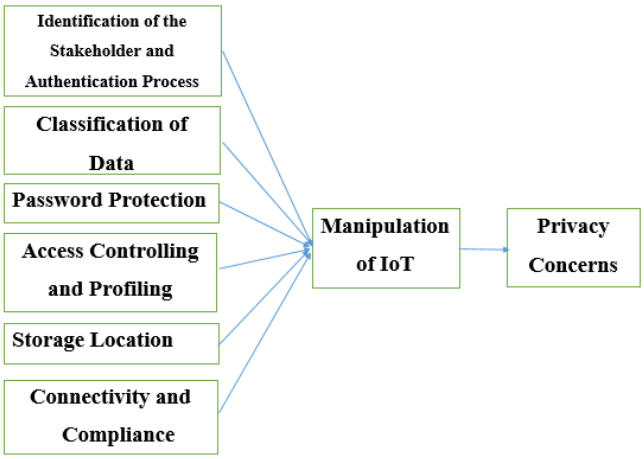

FIGURE 1

THE CONCEPTUAL FRAMEWORK

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

Figure 1 portrays the conceptual model that have been developed based on the relationship between different variables that address the ways manipulation of IoT controls can create an impact over the privacy concerns of the wearable device users. The conceptual model further leads to a set of hypotheses in the context of the current study. A set of independent variables have been identified after an extensive literature review that include the Identification of the stakeholder and authorization process, classification of data, password protection and encryption, access control and profiling, storage location, connectivity and compliance. Manipulation of IoT controls act as a moderating variable that can reflect the extent to which the different privacy controls can be manipulated without compromising the privacy concerns.

The invention of wearable devices and the developments in the IoT has significantly contributed towards benefit of the users, but in the case of health medical sector where these wearable devices act as life savours (Poongodi et al., 2020). However as discussed earlier the privacy concerns of the users of the smart wearable devices are increasing with each passing day since smart device users in the contemporary world are more conscious about privacy of their data and information. In order to achieve the targets of the privacy concerns one needs to figure out the extent to which the IoT controls can be manipulated so that they successfully contribute towards the mentioned objective. This leads to the identification of the privacy control factors that allow the manipulation and ultimately contribute towards the reduction of privacy concerns. The current study has identified a set of most important factors that significantly contribute towards IoT controls' manipulation.

Identification of the Stakeholder and Authentication Process

The foremost factor that contributes towards the reduction of the privacy concerns and allows manipulation of IoT controls is related to the stakeholders and the authentication process. The stakeholders in the context of IoT supported devices can be identified as the smart wearable device users. These stakeholders demand for different levels of privacy controls and varying authentication approaches allowing manipulation of the IoT controls and provision of desired privacy levels to each stakeholder (Putta et al., 2020).

Classification of Data

In the context of privacy, the data is categorized either as sensitive, non-sensitive and moderately sensitive. This classification of data emerges as an important factor for the manipulation of IoT controls and reduces the privacy concerns (Dai et al., 2017). For instance, the data related to the banking and money transactions can be termed as highly sensitive and it requires greater levels of privacy for the services or smart wearable device users.

Password Protection

The password protection techniques are one of the most important factors in the determination of the privacy controls of the smart wearable device users over their data and information. The various approaches to password protection include the combination of alphabets and numbers, biometric recognition and face recognition that are used as device passcodes. These approaches significantly contribute towards the reduction of privacy concerns through their manipulation (Hasan et al., 2020).

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

Access Controlling and Profiling

Controlling the levels of access and making profiles of the smart wearable devices is most often designated as one of the key contributors towards reduction in privacy concerns (Fiandrino, et al., 2019). Most often the wearable device users demand for higher levels of access and profiling controls that might result into manipulation of IoT controls. Manipulation of the different authorization levels and profiling approaches not only secures the data but also enhances the effectivity of wearable devices in terms of providing access to the relevant data concerning the device user.

Storage Location

The storage locations are also identified as one of the key factors that serve the purpose of reduction in privacy concerns if handled properly. It enables the smart wearable device users to have understanding about the locations where the data could be stored and thus the user could restrict the storage locations because of the upsurge in redundancy (Banerjee, Hemphill, & Longstreet, 2017). Nonetheless, storing the information in various locations assists to have back up yet also increases the attack surface if the data could be controlled through any storage location.

Connectivity and Compliance

Smart wearable devices should ensure that its compliance is associated with such governing and regulatory bodies that users feel safe and protected while sharing their data. Whereas, the connectivity of the devices should also depend on the trust and reliability that users can connect with other devices with proper comfort and ease. The access to the high-speed internet facility and the regulations focusing privacy controls require higher levels of manipulation of IoT controls ultimately creating an impact over reduction in privacy concerns. Thus, this factor also strongly relates to the reductions in privacy concerns (Celic & Magjarevic, 2020).

HYPOTHESES

The mentioned hypothesis highlights one of the important aspects of piracy concerns in IoT supported wearable devices. Since the manipulation of the privacy controls can serve the privacy concerns up to some extent however it does not always the serve the privacy purpose. For instance, the manipulation of the IoT controls at times reduces the storage burdens but over manipulation can sometime results into inefficiency of wearable device and enhances security concerns. Therefore, it can both positively and negatively affect the privacy concerns.

H1: Identification of stakeholders and authentication process significantly contributes towards the manipulation of IoT controls.

The stockholders in IoT in form of wearable device users, manufactures, and cloud service providers significantly contribute towards the manipulation of IoT controls. On a similar note, the different cloud service providers and manufacturers of smart devices can come up with varied authentication processes that significantly contribute towards the manipulation of IoT controls (Abdul-Ghani & Konstantas, 2019).

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

H2: Classification of Data significantly contributes towards the manipulation of IoT controls.

In the context of the privacy concerns related to wearable devices the data classification is termed as the very sensitive data, moderately sensitive data, and not sensitive data. This classification leads to the manipulation of IoT controls since high sensitive data might require manipulation of IoT controls in a way that it leads reduction in privacy concerns up to a great extent (Li et al., 2019).

H3: Password protection and encryption significantly contribute towards the manipulation of IoT controls.

Password protection and encryption are the two important tools for data security and privacy in a cloud environment. The tools depict a strong relationship with the levels of manipulation that can be made to IoT controls and control the reduction and increase of privacy concerns in smart wearable devices (Ali & Awad, 2018).

H4: Profiling and access controlling significantly contribute to the manipulation of IoT controls.

The level of access and privileges granted to the user of wearable devices in terms of profiling and control levels also strongly relates to manipulation of IoT controls. The greater levels of authorization require high rates of manipulation in IoT controls in a way that it also ensures the data security and privacy of the wearable device users (Blythe & Johnson, 2019).

H5: Storage location significantly contributes to the manipulation of IoT controls.

Storage location refers to the wearable device ability to store the data in multiple locations. In the context of IoT, the three important locations are cloud storage, mobile storage, and device storage (Shafagh et al., 2017). All three types of storage location create a strong impact on the manipulation of IoT controls. The greater levels of storage capacities allow greater extents of manipulation ultimately contributing towards the reduction or increase in privacy concerns.

H6: Connectivity and Compliance significantly contribute to the manipulation of IoT controls.

The connectivity and compliance feature strongly relate to the manipulation of the IoT controls. For instance, the slow connectivity and strict regulations concerning the data security in IoT supported devices might allow less manipulation control and ultimately lead to either the increase or reduction in privacy concerns (Barati et al., 2020).

METHODOLOGY

Item Development

A survey that involved variables for the hypothesis definite within the conceptual model was conducted to gather information, which could be utilised to empirically analyse the hypothesis of the research. However, to assure the validity of the content, the variables were generated based on a comprehensive questionnaire associated with prior privacy studies. A Likert scale was included to conduct the survey with answers ranging from "1. Strongly disagree to 5. Strongly agree." For analysing the data appropriately and effectively, some experienced and skilled people were invited to test the results efficiently. Moreover, there are a total of six factors

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

or ways through which IoT controls can be manipulated to observe the effect on privacy concerns and risk to the privacy of the data related to patients. The study targeted wearable devices form different age groups and the questionnaire was designed in a way that it covers responses for all the factors that are involved in the reduction of the privacy concerns of the wearable device user.

Study Design and Procedure

The survey was conducted over social media, since the participants of the research were healthcare wearable devices' users. Initially, the participants were needed to sign the consent form, by going through it thoroughly. However, there were 250 respondents who participated in the survey. In addition, after collecting the data Correlation analysis was performed to relate the demographics of the respondents of the groups. The correlation results depicted that the identified factors such as the Identification of the stakeholder and authorization process, classification of data, password protection and encryption, access control and profiling, storage location, and connectivity and compliance and their manipulation significantly contribute towards the reduction of privacy concerns of the smart wearable device users.

RESULTS

Scale Development

For the purpose of testing the hypothesis, the data was collected through the use of close-ended survey that included scales for the variables or constructs mentioned in the research model. The scale developed in this research was based on the extensive preliminary review of the literature and survey related to the phenomenon being investigated. For instance, the items measuring the construct of manipulation were measured by seven questions, which were extracted and adapted from numerous peer-reviewed articles (Taylor, Reilly & Lempereur, 2017). On a similar note, while taking in account the relationship between the identification of the stakeholders'/authentication process and privacy control, a variable was designed to observe this aspect of privacy control (Abdul-Ghani & Konstantas, 2019). This construct was measured with the help of three different questions that assessed the strength of the relationship between two variables based on the perceptions of research participants. The relationship between classification of data and privacy control was measured by designing three relevant questions extracted from the information conveyed with reference to the strength of bonding between the classification of data and privacy control in smart wearable devices (de Morais, Sadok, & Kelner, 2019). Research has highlighted the efficiency of password protection and encryption in IOT based smart wearable devices. A section containing three questions referred to this aspect of privacy control in the survey questionnaire (Sinha & Sheel, 2017). It was identified that the access control and profiling remains an important aspect in privacy control (Pinno, Grégio, & De Bona, 2020). In the light of this argument a set of three questions were developed to further investigate the relationship between the two constructs. Storage location in from of the cloud and device storage significantly contributes toward the manipulation of privacy controls (Santos et al., 2017). The findings of the authors are further extended for interrogation through set of three questions in the survey questionnaire which seek to measure the importance of storage location from the perspective of smart wearable device users. It was argued in his research that the internet connectivity and compliance plays a key role in governing the privacy of smart wearable

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

device users (Autry, 2019). In order to further explore the impact of connectivity and compliance over the privacy control on of sections the survey questionnaire asks for three responses from smart wearable device users. Finally, the assessment of the privacy concerns of smart wearable device users was addressed through three questions related to reductions in privacy controls based on the research performed by (Krafft, Arden, & Verhoef, 2017).

Survey Administration

Survey administration remains an important aspect with reference to the reliability and quality of the quantitative research. The reponses collected from the research participants were checked for validity and bogus responses were separated from those which were valid (Wilson, Srite, & Loiacono, 2017). As a result of this process a total of 250 responses were considered for empirical evaluation. The biasness in the responses was assessed based on the validity of information provided and seeking opinions from the experts in information technology regarding the responses that were subjected to biasness. It was ensured during the survey that all the research participants have experience of using smart wearable device and they have basic knowledge of privacy concerns associated to the devices that they use (Table 1).

TABLE 1
SURVEY ADMINISTRATION

Variable	Sources	Number of Items
Manipulation of IoT Controls	Taylor et al., 2017	7
Stakeholder Identification and Authentication Process	Abdul-Ghani & Konstantas, 2019	3
Classification of Data	de Morais et al., 2019	3
Password Protection	Sinha & Sheel, 2017	3
Access Controlling and Profiling	Santos et al., 2017	3
Storage Location	Santos et al., 2017	4
Connectivity and Compliance	Autry, 2019	3
Privacy	Krafft et al., 2017	3

The questionnaire was initially used for pilot testing. A total of 250 undergraduate and graduate students participated in the survey. Their feedback was analysed and changes were made. After that, the questionnaire was distributed for data collection. A total of 250 responses were received out of which no questionnaire was incomplete, so a total of 250 responses were considered for the study. Table 2 provides respondent demographics.

TABLE 2
GENDER: AGE CROSSTABULATION

Gender	Age					Total
	20-25	36-30	31-35	36-40	41 and Above	
Male	81	14	5	1	0	101
Female	124	13	7	2	3	149
Total	205	27	12	3	3	250

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

The demographics show that 101 males and 149 females participated in the survey. Analysing the above table, we can conclude that all the respondents were over 20 years of age and all the males were less than 41 years of age.

Measurement Model and Internal Consistency

The eminence of the measurement model is usually evaluated in terms of its content validity, construct validity, and reliability. Content validity is defined as the degree to which the items represent the construct being measured. Content validity is usually assessed by the domain experts and literature review. The reliability of the measurement addresses the concern of how well the items for one construct correlate or move together. Reliability is usually assessed by Cronbach's alpha. Cronbach's is a measure of internal consistency among all items used for one construct. The Cronbach's alpha was the study was computed and the results are shown in Table 3.

TABLE 3
INTERNAL CONSISTENCY

Cases	**Number of Items**	**0%**
Valid	250	100.0
Excluded	0	0.0
Total	250	100.0
Reliability Statistics		
Cronbach's Alpha	Number of Items	
0.948	29	

The value of Cronbach's alpha should be greater than 0.7 to be acceptable. The reliability test for the study is 0.947 which shows that all the items are consistent. This reflects that the questionnaire is internally consistent and can produce valuable results as per the purpose and objectives of this research (Table 3).

DISCUSSION

The correlation results for the survey conducted are depicted in Appendix A. The results unveil some important facts about the privacy control factors that can reduce or enhance the privacy controls in smart IoT based wearable devices. The table depicts the p values for each pair of factors considered in the study. It can be observed that the all the relationships are positive while p values in the range of +0.30 demonstrate a weak relationship, the values around +0.50 demonstrate moderate relationships and values in the range of +0.70 reveal a strong relationship between the variables.

The results for the manipulation of IoT controls reveal that it had a moderate relationship with the factors related to the identification of the stakeholder and authentication process, classification of data, password protection, internet connectivity, and compliance. Meanwhile, a weak relationship can be observed in relation to the storage location and privacy control. For instance, it can be observed that Pearson correlation values for stakeholder and authentication process, classification of data, password protection, internet connectivity, and compliance are 0.674, 0.614, 0.642, 0.629, 0.444, 0.529, and 0.443 respectively and reflect their reliance over the manipulation of IoT controls.

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

The survey results in the context of the identification of the stakeholder and authentication process revealed that it has a moderate relationship with certain the other factors such as the classification of the data, password protection, internet connectivity, and manipulation of IoT controls. A weak to the strong relationship between the variables was identified based on the aforementioned values. For instance, stakeholders' Pearson correlation value with password protection showed a comparatively stronger relationship; whereas the relationship was weak with privacy.

The classification of data can also be observed as an important factor that can be manipulated to reduce privacy concerns among the smart wearable device users. The survey results revealed that this factor has a strong relationship with other factors considered in the study such as access controlling and profiling and password protection. However, certain factors such as identification of stakeholders, classification of data and internet connectivity depict a moderate relationship with this variable. The mentioned argument can be justified through the Pearson correlation values for the respective variables. For instance, Pearson correlation values for the relationship between the classification of data and access to control and profiling was higher and this justifies the strong relationship between the factors. It has further been revealed that access control and profiling plays a significant role in the manipulation of IoT controls that ultimately reduction of privacy concerns among the users of the device. However, the factor significantly relies on the manipulation of certain other factors as depicted by the correlation results in Appendix A (Figure A1; Table A1).

Access control and profiling have been reported as an important manipulation factor for reducing privacy concerns among smart wearable device users in a number of studies. The correlation statistics for the current study reveals that it has a strong relationship with the classification of data. However, the variable depicts the moderate and weak relationship with certain other factors such as stakeholder identification and authentication, password protection, storage location and internet connectivity. Therefore, to reduce privacy concerns through access control and profiling classification of data remains a key factor.

The survey results revealed that the storage location carries a moderate or weak relationship with other factors such as the stakeholder identification and authentication, classification of data, access controlling and profiling, and internet connectivity. However, it was observed that if the reduction of the privacy concerns is targeted via this factor its relationship with the classification of data remains very significant. Due to the reason that it shows a comparatively strong relationship with password protection with reference to the aforementioned criteria of assessing the Person correlation value that comes out to be 0.668.

The factor of internet connectivity and its speed also remains a key factor in the achievement of the privacy concern reduction targets in smart wearable devices (Pouraghily, et al., 2018). In the context of the current study, the survey results shown in Appendix A reflects that internet connectivity has a moderate relationship with most of the factors such as the stakeholder identification and authentication, classification of data, password protection, access control profiling while showing a weak relationship with the storage location. Therefore; it can be argued that the manipulation of this factor to reduce privacy concerns requires the consideration of a number of other mentioned factors. The Pearson correlation values further reveal that the privacy controls have a strong relationship with password protection.

Concisely, it can be argued that the reduction of privacy concerns emerges as a complex task due to its reliability over a number of other factors and their mutual relationship.

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

CONCLUSION

The above study concludes that there are a number of privacy control variables that contribute towards the reduction of privacy concerns among the IoT based smart wearable device users. The study focused on some important factors identified from the literature in form of identification of the stakeholder and authorization process, classification of data, password protection, and encryption, access control and profiling, storage location, and connectivity and compliance. The survey results for the mentioned control variables reflected that due to its reliability of privacy concerns over a number of factors and their mutual relationship the reduction of privacy concerns remains a tough job. The classification of data, password protection and stakeholder identification and authentication can be identified as some important factors based on the results of the study.

FUTURE RESEARCH

The current research being conducted is limited in terms of scope and application; for instance, this research has only offered empirical analysis, but has inefficiently presented in-depth analysis of the key factors in the manipulation of IoT wearable devices. At the same time, this research cannot be possibly considered applicable without sufficient knowledge resulting from the experience of the medical and nursing staff within the healthcare sector, which means that there is significant potential for future researchers; for instance, they can consider greater number of sample participants for the research, and can explore into different aspects that can directly and indirectly contribute in reduced privacy concerns.

REFERENCES

Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22.

Aldwairi, M., & Tawalbeh, L. A. (2020). Security techniques for intelligent spam sensing and anomaly detection in online social platforms. *International Journal of Electrical and Computer Engineering*, *10*(1), 275.

Alharbi, R., & Almagwashi, H. (2019). The Privacy requirments for wearable IoT devices in healthcare domain. In *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 18-25. IEEE.

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, *18*(3), 817.

Amyx, S. (2017). Privacy dangers of wearables and the internet of things. In *Managing Security Issues and the Hidden Dangers of Wearable Technologies* 131-160. IGI Global.

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, *1*(2), 99-109.

Autry, T. (2019). *Secure IoT Compliance Behaviors Among Teleworkers* (Doctoral dissertation, Capella University).

Banerjee, S. S., Hemphill, T., & Longstreet, P. (2017). Is IOT a threat to consumer consent? The perils of wearable devices' health data exposure. *The Perils of Wearable Devices' Health Data Exposure*.

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 49-57.

Barati, M., Rana, O., Petri, I. and Theodorakopoulos, G. (2020). GDPR compliance verification in Internet of Things. *IEEE Access*, 8, pp.119697-119709.

Bhatt, S., Patwa, F., & Sandhu, R. (2017). An access control framework for cloud-enabled wearable internet of things. In *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, 328-338. IEEE.

Blythe, J. M., & Johnson, S. D. (2019). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 1-29.

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

Celic, L., & Magjarevic, R. (2020). Seamless connectivity architecture and methods for IoT and wearable devices. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *61*(1), 21-34.

Dai, W., Qiu, M., Qiu, L., Chen, L., & Wu, A. (2017). Who moved my data? privacy protection in smartphones. *IEEE Communications Magazine*, *55*(1), 20-25.

de Morais, C. M., Sadok, D., & Kelner, J. (2019). An IoT sensor and scenario survey for data researchers. *Journal of the Brazilian Computer Society*, *25*(1), 1-17.

Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication. *IEEE Access*, *8*, 60539-60551.

Fiandrino, C., Allio, N., Kliazovich, D., Giaccone, P., & Bouvry, P. (2019). Profiling performance of application partitioning for wearable devices in mobile cloud and fog computing. *IEEE Access*, *7*, 12156-12166.

Hasan, N., Chamoli, A., & Alam, M. (2020). Privacy challenges and their solutions in IoT. In *Internet of Things (IoT)*, 219-231. Springer, Cham.

Kowatsch, T., & Maass, W. (2012, September). Critical privacy factors of internet of things services: An empirical investigation with domain experts. In *Mediterranean Conference on Information Systems*, 200-211. Springer, Berlin, Heidelberg.

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions?. *Journal of Interactive Marketing*, *39*, 39-54.

Li, F., Lee, C. H., Chen, C. H., & Khoo, L. P. (2019). Hybrid data-driven vigilance model in traffic control center using eye-tracking data and context data. *Advanced Engineering Informatics*, *42*, 100940.

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.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1636-1675.

Markets and Markets, 2020. Wearable device market. Retrieved July 2, 2021, from https://www.marketsandmarkets.com/Market-Reports/wearable-medical-device-market-81753973.html?gclid=CjwKCAiA7939BRBMEiwA-hX5J7hanLpCLeK-8AoW-gOz61A2nA5NoesTEFUcg-fRBVp2kkSZmAbP-hoCjOYQAvD_BwE

Meng, Y., Zhang, W., Zhu, H., & Shen, X. S. (2018). Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *IEEE Wireless Communications*, *25*(6), 53-59.

Parashar, R. (2016). Security and privacy issues in internet of things. *Global Sci-Tech*, *8*(4), 233-242.

Pinno, O. J. A., Grégio, A. R. A., & De Bona, L. C. (2020). ControlChain: A new stage on the IoT access control authorization. *Concurrency and Computation: Practice and Experience*, *32*(12), 5238.

Poongodi, T., Krishnamurthi, R., Indrakumari, R., Suresh, P., & Balusamy, B. (2020). Wearable devices and IoT. In *A handbook of Internet of Things in biomedical and cyber physical system* 245-273. Springer, Cham.

Pouraghily, A., Islam, M. N., Kundu, S., & Wolf, T. (2018). Privacy in blockchain-enabled iot devices. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 292-293. IEEE.

Putta, S. R., Abuhussein, A., Alsubaei, F., Shiva, S., & Atiewi, S. (2020). Security benchmarks for wearable medical things: stakeholders-centric approach. *In Fourth International Congress on Information and Communication Technology*, 405-418. Springer, Singapore.

Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2018). Challenges of securing Internet of Things devices: A survey. *Security and Privacy*, *1*(2), e20.

Santos, J., Wauters, T., Volckaert, B. and De Turck, F. (2017). Resource provisioning for IoT application services in smart cities. In 2017 13th International Conference on Network and Service Management (CNSM) 1-9. IEEE.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable storage and sharing of iot data. In *Proceedings of the 2017 on Cloud Computing Security Workshop* 45-50.

Siby, S., Maiti, R. R., & Tippenhauer, N. O. (2017). IoTScanner: Detecting privacy threats in IoT neighborhoods. In *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security* 23-30.

Sinha, A., & Sheel, V. (2017). *U.S. Patent No. 9,773,119*. Washington, DC: U.S. Patent and Trademark Office.

Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

Taylor, M., Reilly, D., & Lempereur, B. (2017). An access control management protocol for Internet of Things devices. *Network Security*, *2017*(7), 11-17.

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

Thierer, A. D. (2014). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Rich. JL & Tech.*, *21*, 1.

Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Adam Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, *21*.

Wilson, E. V., Srite, M., & Loiacono, E. (2017). A call for item-ordering transparency in online IS survey administration.

Yildirim, H., & Ali-Eldin, A. M. (2019). A model for predicting user intention to use wearable IoT devices at the workplace. *Journal of King Saud University-Computer and Information Sciences*, *31*(4), 497-505.

Zhu, L., Gai, K., & Li, M. (2019). Security and privacy issues in internet of things. In *Blockchain Technology in Internet of Things*, 29-40. Springer, Cham.

APPENDIX A

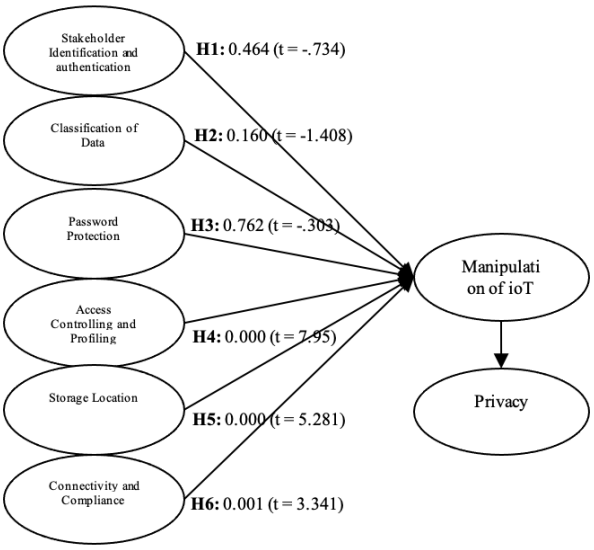

FIGURE A1
HYPOTHESIS IN THE STUDY

TABLE A1
RESULT OF IOT MANIPULATION
HYPOTHESIS SUMMARY

Hypothesis	Significant value	Result
Identification of stakeholders and authentication process significantly	0.464 (t = -.734)	Rejected
Classification of Data significantly contributes towards the manipulation of IoT controls.	0.160 (t = -1.408)	Rejected
Password protection and encryption significantly contribute towards the manipulation of IoT controls.	0.762 (t = -.303)	Rejected

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.

Profiling and access controlling significantly contribute to the manipulation of IoT controls.	0.000 (t = 7.95)	Accepted
Storage location significantly contributes to the manipulation of IoT controls.	0.000 (t = 5.281)	Accepted
Connectivity and Compliance significantly contribute to the manipulation of IoT controls	0.001 (t = 3.341)	Accepted

Citation Information: Suhluli, S. (2021). The impact of manipulating IOT wearable controls on users privacy concerns. *Journal of Management Information and Decision Sciences, 24*(S3), 1-16.