Proceedings of 6th International Conference of Economic, Business and Government Challenges 2023. Vol. 6 No. 1 October 2023: 233-241

Awareness of IoT with Safeguarding Personal Data in the Connected World

Hanis Haidar Abdul Karim[1], Nor Syifaa Nasuha Aziz[2], Natasha Afina Salem[3], Amri Mohamad[4*]
Universiti Teknologi MARA Cawangan Kelantan, Malaysia[1,2,3,4]
amri093@uitm.edu.my[4*]

Abstract: IoT technology has transformed our daily lives and quality of life by providing convenience and efficiency at the same time. This research investigates the level of knowledge and understanding regarding the Internet of Things (IoT) in relation to safeguarding personal data. A sample was selected from the target population of IoT users. A total of 35 questionnaires were distributed to Malaysian citizens using simple random sampling methods to achieve the research objectives. The findings suggest a positive correlation between the perceived usefulness and the level of awareness regarding privacy and security in the context of the Internet of Things (IoT) among the citizens of Malaysia. The perceived usefulness of IoT technology substantially impacts users' level of awareness regarding privacy and security concerns. Future research on the effectiveness of different strategies in promoting IoT privacy and security awareness among individuals in other countries with similar cultural contexts is essential.
Keywords: Internet of Things (IoT), Awareness, Safeguarding personal data, cyber security

I. Introduction

The term "Internet of Things" (IoT) pertains to a network of tangible entities or objects that are equipped with sensors, software, and other technological components, enabling them to establish connections and exchange data with other devices and systems via the Internet, according to Alexander (2022). The spectrum of these devices encompasses both minimal domestic appliances and intricate industrial machinery. The potential of the IoT to bring about groundbreaking changes in our lifestyles and occupations through the enhancement of automation, efficiency, and connectivity cannot be underestimated. As per the online resource titled "What Is the Internet of Things (IoT)?" The term "Internet of Things" (IoT) encompasses a network of tangible entities, commonly referred to as "things," which are equipped with sensors, software, and other technological components. These elements enable seamless communication and data interchange with other systems and devices via the Internet. The range of objects encompasses both everyday household items and proficient industrial equipment. The current number of interconnected Internet of Things (IoT) devices exceeds seven billion, and it is projected to reach 10 billion by 2020 and 22 billion by 2025. This number demonstrates the significance of the IoT as a critical player in the technological revolution of this decade.

IoT enables communication between devices and users. Information and control are now accessible to individuals who want to improve their lives (Mohamed, 2019). Also, IoT technology has the potential to improve businesses, cut costs and improve customer satisfaction. Real-time sensors that monitor machinery output at a factory can help to optimise maintenance schedules and minimise unplanned downtime devices typically operate and configure themselves independently, lasting for extended periods on their energy sources, allowing organisations to avoid manual maintenance and replacement of devices. Moreover, IoT devices can be analysed to understand customer behaviour and preferences, which can then inform business decisions and enhance the quality of products and services. As a result, the Internet of Things can bring about sweeping industry changes and improve the lives of millions by providing cost-effective and efficient solutions.

Effective communication is a crucial aspect of IoT, as it allows for consistent quality of service and interaction with other devices or platforms across multiple networks. Unfortunately, their security and privacy weaknesses are widely recognised (Mohamed, 2019). Both individuals and businesses are at risk of being harmed by these vulnerabilities, which can lead to the theft of sensitive information. Implementing strict security measures and protocols is essential to mitigate risks and ensure the safe use of IoT devices. However, securing IoT devices and services is difficult due to their limited power and computing resources and frequent use of wireless communications (Tawalbeh & Zawika, 2020).

Additionally, the diversity of IoT devices and their applications adds complexity to the security landscape. A multi-layered approach that includes network segmentation, access control, encryption, and regular software updates is necessary to address these challenges and protect against potential threats. Furthermore, continuous monitoring and threat intelligence gathering can help promptly detect and respond to security incidents. Consequently, the absence or limited presence of controls renders these devices vulnerable to attacks (Alladi et al., 2020).

II. Literature Review

Awareness of IoT Privacy and Security

Awareness refers to individuals' cognitive grasp and comprehension of the potential risks and benefits of Internet of Things (IoT) devices. It is vital to raise awareness among users about the potential security and privacy risks associated with IoT devices and the steps they can take to protect themselves. By doing so, users can make informed decisions about IoT devices and take appropriate measures to safeguard their personal information. Furthermore, by being aware of IoT privacy and security, individuals can contribute to developing better security measures and standards for IoT devices, ultimately benefiting the entire industry and society.

Manufacturers and policymakers must prioritise security and privacy in designing and regulating IoT devices. However, user education and awareness are equally important in ensuring a safe and secure IoT ecosystem. Some argue that it is not solely the responsibility of individuals to ensure IoT security, as manufacturers and policymakers should bear the majority of the burden in implementing effective security measures. For instance, in healthcare, IoT devices like pacemakers and insulin pumps can be hacked and manipulated, causing harm to patients. Manufacturers and policymakers must ensure these devices have stringent security measures to prevent such attacks. Nevertheless, individuals must be educated on safeguarding their personal information and using their devices safely to avoid potential risks.

Nevertheless, individuals can take steps to protect themselves, such as regularly updating device software and using strong passwords. Furthermore, it is imperative to foster collaboration among all relevant parties to effectively tackle the intricate and dynamic security challenges that arise from the extensive integration of Internet of Things (IoT) gadgets.

TAM Model

Fred Davis initially proposed the Technology Acceptance Model (TAM) in 1986. The Technology Acceptance Model (TAM) is a conceptual framework that aims to elucidate the factors influencing users' acceptance of information systems or technologies (Saenpon, 2017). This technology has been extensively employed across diverse domains, encompassing the Internet of Things (IoT). The Technology Acceptance Model (TAM) serves as a valuable conceptual framework for comprehending the various factors that influence users' adoption of Internet of Things (IoT) devices. These factors encompass the perceived usefulness of such devices. Manufacturers and policymakers can promote increased adoption of Internet of Things (IoT) devices and prioritise the safety and security of all users by carefully considering these factors and effectively addressing potential barriers.

By acknowledging and mitigating potential obstacles and prioritizing the protection and reliability of these devices, we can foster increased adoption and fully harness the capabilities of the Internet of Things (IoT). A cooperative approach involving industry, government, and individuals will be imperative to accomplish this objective while safeguarding privacy and security.

Perceived Usefulness

Perceived usefulness refers to how individuals believe a particular IoT device will enhance their daily lives. Users who perceive the IoT as applicable are more engaged with privacy and security settings (Sanjit Thapa et al., 2023). They will recognise the importance of protecting their data and maintaining security, as it directly affects the usefulness and functionality of the IoT. This engagement develops a deeper awareness of privacy and security issues.

Furthermore, individuals who perceive the IoT as applicable are more likely to invest time and effort learning about the device's features and capabilities. This knowledge can help them make informed decisions about using the device safely and responsibly. For example, a person who uses an innovative home system to control their locks and security cameras will understand the importance of securing their network and protecting their data. They may use strong passwords, regularly update their software, and monitor their network for unusual activity to ensure their intelligent home system remains secure.

Conceptual Framework

As shown below, this study establishes a relevant conceptual framework and components. Perceived Usefulness (PU) are the independent variables in this study. Therefore, the dependent variable will be awareness of IoT privacy and security. The suggested conceptual framework is presented as in Figure 1 below.

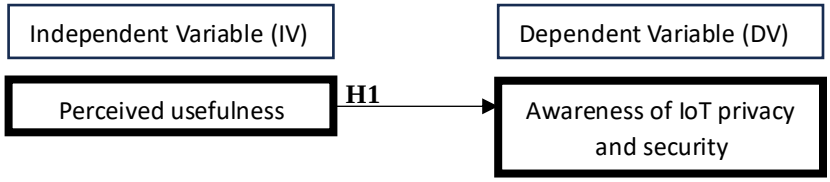

Figure 1. Proposed Conceptual Framework

Hypothesis Development

The relationship between perceived of usefulness and the awareness of IoT privacy and security

The correlation between the perceived usefulness of IoT systems and the level of awareness regarding privacy and security concerns is of utmost importance in developing and widespread adoption of such systems. In other words, the more valuable people perceive IoT technology, the more aware they are of the importance of privacy and security concerning IoT. Several studies have investigated the relationship between perceived usefulness, IoT privacy, and security awareness.

Study by Koohang et al. (2022) revealed a significant correlation between IoT awareness and users' understanding of privacy and security. Furthermore, when people recognise the value and usefulness of IoT technology, they may be more motivated to protect their privacy and ensure the security of their IoT devices and data. According to the study published by Ho-Sam-Sooi et al. (2021), the influence of security and privacy on consumer purchasing behaviour is significant, mainly when consumers are provided with information about privacy and security. Users more aware of IoT devices' potential security and privacy risks may be more likely to prioritise security and privacy when purchasing.

The analysis of the search results reveals a substantial correlation between the perceived usefulness of the Internet of Things (IoT) and the level of awareness regarding its functionalities. The more valuable individuals perceive IoT products and applications to be, the more likely they will have a positive attitude toward and adopt them. Additionally, the level of awareness regarding the Internet of Things (IoT) can impact users' understanding of privacy and security concerns associated with IoT.

H1: There is a positive relationship between perceived usefulness and the awareness of IoT privacy and security

III. Research Method

Population sample

The study's target population comprises individuals actively engaging with Internet of Things (IoT) devices or technology. The term "Internet of Things" (IoT) denotes a network comprised of interconnected devices that engage in data exchange and communication through the utilisation of the Internet. In this context, the population comprises individuals who engage with IoT devices, such as intelligent home systems, wearable devices, or any other form of IoT technology. These individuals may come from various backgrounds and age groups and possess different levels of technological proficiency.

For this study, a sample was selected from the target population of IoT users. A total of 35 questionnaires were distributed to Malaysian citizens who know IoT devices and use them in their daily life using simple random sampling methods to achieve the research objectives. This method was selected to guarantee that every element within the population size is afforded an equitable opportunity for selection. A total of 35 questionnaires were distributed, of which 30 were deemed suitable and utilised for this study.

Data Collection Method

The present study was undertaken to utilise a quantitative research approach, wherein primary data was collected. The primary means of data collection employed in this study involved the utilization of a survey methodology, wherein questionnaires were disseminated to participants for self-administration. The survey will also be administered in the English language. The questionnaire will be distributed via online survey form, electronic mail, and WhatsApp. This quantitative method is used because it collects data quickly and is affordable.

Research Instruments

The questionnaire has been divided into two distinct sections, namely Section A and Section B. The questionnaire consisted of 14 items, with Section A comprising four questions and Section B comprising

ten questions. These questionnaires were distributed daily to Malaysian citizens who utilise Internet of Things (IoT) technology.

The first section, Section A, will include four items related to gender, age, ethnicity, and working sectors, as shown in Table 3.3.1 below. In measuring the responses to a questionnaire, scales ordinal, nominal, ratio, and interval are used.

Table 1. Demographic

Construct	Items	
Demographic	D1	**Gender** Male/Female
	D2	**Age** 20-30/31-40/41-50/51 and above
	D3	**Ethnicity** Malay/Chinese/Indian/Others
	D4	**Working Sectors** Accounting/Banking/Manufacturing/Public Sector/Others

Section B will focus on the dependent variable, the Internet of Things (IoT) privacy and security awareness, as shown in Table 2 below which to assess the level of awareness regarding the intersection of the Internet of Things (IoT) with privacy and security, participants were requested to indicate their level of agreement or disagreement on a Likert scale ranging from 1 to 5. The scale was used to gauge their personal experiences about misusing their personal information, unauthorised access by unidentified individuals, and excessive data collection by IoT devices. Five (5) items were tested to assess the level of awareness among individuals regarding privacy concerns in the context of the Internet of Things (IoT). The questionnaire utilised in this study was adapted from the findings of Adhikari and Panda (2018), with minor adjustments made to suit the specific research context.

Table 2. Dependent Variable

Construct	Items	
DV: Awareness of IoT in privacy and security (Privacy concerns)	DV1	I am concerned that my personal information gathered by IoT devices could be used for wrong purposes.
	DV2	I am concerned that my personal information gathered by IoT devices could be used accessed by unknown parties.
	DV3	I usually think twice before providing my personal information in IoT devices.
	DV4	I feel IoT devices are collecting excessive personal information.
	DV5	I am concerned that my personal information gathered by IoT devices could be used in a manner I am unaware of.

Meanwhile, the next part of the questionnaire asked about independent variables, and the focus was on perceived usefulness, as shown in Table 3.3.3 below. In order to evaluate the perceived usefulness of IoT devices, participants were instructed to indicate their level of agreement or disagreement on a 5-point Likert scale regarding the ease of using these devices in their daily lives. A total of five (5) items were used in order to assess the perceived usefulness of the subject matter. The questionnaire utilised in this study was derived from Davis's (1989) work, with a few minor adjustments made.

Table 3. Independent Variable

Construct	Items	
IV: Perceived Usefulness	IV1	Using IoT devices enables me to accomplish my tasks more quickly.
	IV2	Using IoT devices improves my productivity in my daily life.
	IV3	Using IoT devices enhances my effectiveness in daily tasks.
	IV4	Using IoT devices make my life easier.
	IV5	I find it useful to use IoT devices at home.

Data Analysis

The data analysis was conducted by applying the SPSS software. The questionnaires that were received were evaluated utilising the data analysis methodology. The data in the SPSS software underwent processing through a two-step procedure. During the initial stage, the data were identified and compared to the collected responses' mean. Subsequently, the correlation analysis was performed on the dependent and independent variables using the Statistical Package for the Social Sciences (SPSS).

The information analysis was executed using a descriptive methodology, employing techniques such as frequency analysis, mean calculation, and standard deviation assessment. The mean value signifies the arithmetic average of all participants' responses on the ranking scale. In contrast, the standard deviation indicates the extent to which the responses are dispersed across the scale.

Subsequently, frequency analysis was employed to represent the demographic characteristics of the participants. Furthermore, the statistical measures of mean and standard deviations were employed to illustrate the extent of Malaysians' exposure to awareness of the Internet of Things (IoT) with privacy and security. This analysis was conducted within the Technology Acceptance Model (TAM) framework, which is commonly perceived as a reliable theoretical framework for studying user acceptance of technology.

IV. Results and Discussion

The Statistical Package for Social Science (SPSS) software processed the data analysis. It subsequently proceeds with the presentation of descriptive statistics about the demographic characteristics of the respondents. It is followed by presenting the results obtained from the regression analysis. The outcomes of the hypothesis testing are deliberated upon, and a conclusion is drawn.

Demographic

Table 4. Profiles of Respondents

Profile of Respondents	Frequency	%
Gender		
Male	23	77
Female	7	23
Total	**30**	**100**
Age		
20-30 years old	22	73
31-40 years old	8	27
42-50 years old	-	-
51 years old and above	-	-
Total	**30**	**100**
Ethnicity		
Malay	29	97
Chinese	1	3
Indian	-	-
Others	-	-
Total	**30**	**100**
Working Sectors		
Accounting	7	23
Banking	2	7
Manufacturing	1	3
Public Sector	5	50
Others	15	50
Total	**30**	**100**

The demographic profiles of the respondents who completed the questionnaires are presented in Table 4. This table summarises the characteristics of individuals who utilised the Internet of Things (IoT), including their gender, age, ethnicity, and employment sectors.

Most responses, specifically 23 (77%), were contributed by individuals identifying as women, while the remaining 7 (23%) responses were provided by individuals identifying as men, as determined by gender. The age group with the highest number of recorded individuals was between 20 and 30, comprising 22 individuals, accounting for 73% of the total sample. In contrast, eight individuals, representing 27% of the sample, were over 31. The Malay demographic exhibited the highest participation level, with 29 individuals

representing 97% of the respondents. Table 4 additionally presents the distribution of responses across different working sectors. Among the participants, seven individuals (23%) were employed in the accounting industry, two individuals (7%) were affiliated with the banking industry, one individual (3%) worked in the manufacturing industry, five individuals (17%) were involved in the public sector, and the remaining 15 individuals (50%) were associated with diverse sectors.

Awareness of IoT in Privacy and Security

Table 5. Descriptive Statistics on Awareness of IoT in Privacy and Security

Code	Description	Mean	Variance	Std. Dev	Ranking
DV1	I am concerned that my personal information gathered by IoT devices could be used for wrong purposes.	3.83	1.592	1.262	4
DV2	I am concerned that my personal information gathered by IoT devices could be accessed by unknown parties.	4.03	1.551	1.245	2
DV3	I usually think twice before providing my personal information in IoT devices.	4.23	0.668	0.817	1
DV4	I feel IoT devices are collecting excessive personal information.	3.63	0.654	0.809	5
DV5	I am concerned that my personal information gathered by IoT devices could be used in a manner I am unaware of.	3.97	0.861	0.928	3

Table 5 displays the descriptive analysis of the level of awareness regarding privacy and security in the Internet of Things (IoT) context among individuals residing in Malaysia. A set of five questions was administered in order to assess the dependent variable. The questions utilised in this study were derived from the work of Adhikari and Panda (2018). A five-point Likert scale was administered, ranging from 1 to 5. A score of 1 indicated a strong disagreement with the statement, while a score of 5 indicated a firm agreement. The mean scores displayed above were obtained by calculating the average of each question score.

The three highest mean scores are achieved by DV3, indicating that Malaysians exhibit caution when sharing personal information with IoT devices, with a mean score of 4.23 (std. Dev. = 0.817). It is followed by DV2, where individuals express concern about the potential access of their personal information by unknown parties through IoT devices, with a mean score of 4.03 (std. Dev. = 1.245). Lastly, DV5 reveals that individuals are worried about their personal information being utilised in ways they are unaware of, with a mean score of 3.97 (std. Dev. = 0.928). The findings suggest that Malaysians exhibited a heightened awareness of privacy and security issues related to the Internet of Things (IoT). It was evident in their cautious approach towards sharing personal data, as they expressed concerns about the potential unauthorised access and unfamiliar utilisation of their data.

Based on the data in the table, it is evident that DV1 and DV4 exhibit the lowest mean scores, with values of 3.83 and 3.63, respectively. These scores are accompanied by standard deviations of 1.262 and 0.809, respectively. Instances of privacy concerns related to IoT devices are relatively infrequent. These concerns primarily revolve around the potential misuse of personal information collected by such devices and IoT devices' perceived over-collection of personal data.

Regression Analysis Findings

Table 6. ANOVA for Predictor Perceived Usefulness

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	1.704	1	1.704	2.97	.096b
Residual	16.068	28	0.574		
Total	17.772	29			
a. Dependent Variable: DV					
b. Predictors: (Constant), PU					

The hypotheses formulated in the preceding chapter have been subjected to empirical examination in this study. Before conducting a regression analysis, it is imperative to ascertain the validity of the

independent variables employed in evaluating their association with the dependent variable (Pallant, 2010). In the context of ANOVA, the statistical significance level of 1 percent is represented in Table 4.4.1 ($F = 2.970$, $p = 0.096$).

Based on the findings presented in this analysis, it can be inferred that at least one independent variable influences the dependent variable. Hence, the perceived usefulness (PU) independent variable influences the awareness of privacy and security in the context of this study on the Internet of Things (IoT).

Table 7. Linear Regression (Awareness of IoT in Privacy and Security)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.31	0.096	0.064	0.75753

Table 8. Coefficients for Perceived Usefulness (PU)

Model	IV	Unstandardized Coefficients	Std. Error	Standardized Coefficients	Sig.
1	Perceived Usefulness (PU)	0.37	0.215	0.31	0.096

In statistical analysis, it is of utmost importance to comprehend the association between predictor variables and dependent variables to derive significant and valid conclusions. The analysis includes;

1. the estimation of a coefficient,
2. the calculation of its standard error,
3. the determination of the standardised coefficient (Beta), and
4. the assessment of the p-value.

Through the analysis of these statistical measures, valuable insights can be obtained regarding the potency, significance, and influence of the predictor variable on the dependent variable. Examining the predictor variable (PU) demonstrates a coefficient of 0.370, signifying a positive correlation with the dependent variable. Furthermore, the standardized coefficient (Beta) of 0.310 indicates a moderate effect size. It means that a one-unit increase in PU is associated with a 0.310 standard deviation increase in the dependent variable. Nevertheless, the obtained p-value of 0.096 suggests that the observed relationship lacks statistical significance compared to the commonly accepted threshold of 0.05. Hence, the analysis presented in this study reveals a correlation between PU and the dependent variable. However, it is essential to conduct further research or consider additional variables to establish a statistically significant relationship. Therefore, hypothesis H1 is deemed to be accepted.

V. Conclusion

This study aims to test the relationship between one item in the TAM model, namely perceived usefulness and awareness of IoT privacy and security. Each of the research inquiries in this investigation has been addressed. The study's research questions encompass the following:

1. How much is the public aware of IoT security and privacy?
2. Is perceived usefulness a factor in users' awareness of IoT security and privacy?

In general, the findings of the analysis suggest a positive correlation between the perceived usefulness and the level of awareness regarding privacy and security in the context of the Internet of Things (IoT) among the citizens of Malaysia. This finding indicates that the perceived usefulness of IoT technology substantially impacts users' level of awareness regarding privacy and security concerns. Furthermore, the research revealed that individuals with a strong perception of the Internet of Things (IoT) as highly beneficial were more inclined to possess awareness regarding the potential risks to privacy and security that are linked to it. The findings above underscore the significance of considering the perceived usefulness factor during the design and implementation phases of Internet of Things (IoT) systems to guarantee sufficient privacy and security measures.

Further investigation is required to examine these potential factors and their influence on individuals' awareness of privacy and security in the Internet of Things (IoT) context. Moreover, it should be noted that the results obtained from this analysis are likely to apply only to the population of Malaysia, and caution should be exercised when attempting to extrapolate these findings to other nations or cultural contexts. Hence, it is advisable to exercise caution when extrapolating these findings to different contexts.

The study's theoretical contribution lies in its emphasis on the significance of individual awareness and understanding of privacy and security in Malaysia's context of the Internet of Things (IoT). This contribution adds to the existing body of literature on the subject. It underscores the necessity of implementing focused educational initiatives and policy interventions to tackle these concerns effectively. Additionally, this study opens up avenues for future research on the effectiveness of different strategies in promoting IoT privacy and security awareness among individuals in other countries with similar cultural contexts.

References

Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviours in Social Networks. *Journal of Global Marketing*, *31*(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

Field, A., Miles, J., & Field, Z. (2012). *Discovering statistics using R*. Sage.

Gillis, Alexander. "What Is Iot (Internet of Things) and How Does It Work?" *IoT Agenda*, Mar. 2022, www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.

Ho-Sam-Sooi, Nick, et al. "Investigating the Effect of Security and Privacy on IoT Device Purchase Behaviour." *Computers & Security*, vol. 102, Mar. 2021, p. 102132, https://doi.org/10.1016/j.cose.2020.102132.

INTERNET OF THINGS (IoT) - SECURITY MANAGEMENT. (2018). Malaysian Communications and Multimedia Commission (MCMC). Retrieved June 28, 2023, from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G013_2018_IoT_SECURITY-MANAGEMENT.pdf

Jaspers, E., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, *142*, 255–265. https://doi.org/10.1016/j.jbusres.2021.12.043

Joshi, S. (2023, June 15). *70 IoT Statistics to Unveil the Past, Present, and Future of IoT*. Learn Hub. Retrieved June 25, 2023, from https://learn.g2.com/iot-statistics#:~:text=A%20striking%2098%25%20of%20IoT,as%20their%20most%20critical%20concern

Kleinbaum, D. G., Kupper, L. L., Nizam, A., & Rosenberg, K. E. (2020). *Applied regression analysis and other multivariable methods*. Cengage Learning.

Koohang, Alex, et al. "Internet of Things (IoT): From Awareness to Continued Use." *International Journal of Information Management*, vol. 62, Feb. 2022, p. 102442, https://doi.org/10.1016/j.ijinfomgt.2021.102442.

MCMC IOT - Technical Regulatory Aspects & Key Challenges. (2018, March 30). Malaysian Communications and Multimedia Commission (MCMC). Retrieved June 28, 2023, from https://www.mcmc.gov.my/skmmgovmy/files/20/203a1c3e-3284-4186-ba8f-8cb3df165efd/files/assets/basic-html/page-39.html#

Ogonji, M. S., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of the Internet of Things. *Computer Science Review*, *38*, 100312. https://doi.org/10.1016/j.cosrev.2020.100312

Saenphon, Thirachit. "An Analysis of the Technology Acceptance Model in Understanding University Student's Awareness to Using Internet of Things." *Proceedings of the 2017 International Conference on E-Commerce, E-Business and E-Government - ICEEG 2017*, 2017, https://doi.org/10.1145/3108421.3108432.

Schuster, F., & Habibipour, A. (2022). Users' Privacy and Security Concerns that Affect IoT Adoption in the Home Domain. *International Journal of Human–Computer Interaction*, 1–12. https://doi.org/10.1080/10447318.2022.2147302

Smith, W., & Davis, J. (2018). Introduction to business statistics. World Scientific Publishing.

Statista. (2023, \March 31). *Global IoT cybersecurity concerns 2019, by category*. https://www.statista.com/statistics/1202640/internet-of-things-security-concerns/

Suman, T. (2022). A Review of Internet of Things Application in Malaysia. *Borneo Journal of Sciences & Technology, 4(1),* 70–79. https://doi.org/10.3570/bjost.2022.4.1-11

Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2019). *Using multivariate statistics*. Pearson.

Thapa, Sanjit, et al. "Security Risks and User Perception towards Adopting Wearable Internet of Medical Things." International Journal of Environmental Research and Public Health, vol. 20,no.8,14Apr.2023,p.5519,researchdirect.westernsydney.edu.au/islandora/object/uws:68265/datastream/PDF/view, https://doi.org/10.3390/ijerph20085519. Accessed 31 May 2023.

Unwin, A. (2013). Discovering Statistics using R by Andy Field, Jeremy Miles, Zoë Field. *International Statistical Review*, *81*(1), 169–170. https://doi.org/10.1111/insr.12011_21

What is the Internet of Things (IoT)? (n.d.). Retrieved June 25, 2023, from https://www.oracle.com/internet-of-things/what-is-iot/