Issues in Information Systems
Volume 24, Issue 2, pp. 191-202, 2023

DOI: https://doi.org/10.48009/2_iis_2023_116

Internet of Things (IoT): users' concerns about privacy and security

Alex Koohang, *Middle Georgia State University, alex.koohang@mga.edu*
Carol Springer Sargent, *Mercer University, sargent_cs@mercer.edu*
David Fuller, *Middle Georgia State University, david.fuller@mga.edu*
Tara Underwood, *Middle Georgia State University, tara.underwood@mga.edu*

Abstract

This study investigated users' IoT privacy and security concerns. The study looked at several variables, including job level, daily use of IoT, daily time spent using IoT, age, and gender. Data were collected from employees in various organizations using an instrument with two constructs. The findings showed that older workers in higher job levels and more frequent IoT users had significantly deeper IoT privacy concerns. Additionally, higher job levels and frequency of IoT use significantly influenced employees' security concerns. The implications of the findings are discussed, and recommendations for further research are given.

Keywords: Internet of Things, IoT privacy concerns, IoT security concerns, job level, daily use of IoT, daily time spent using IoT

Introduction

The Internet of Things (IoT) is a rapidly growing technology that has changed how we interact with our everyday environment. It has enabled us to collect and share data, control devices, and even manage our home environment with a button (Bastos et al., 2018). It has been described as one of the most unique disruptive technologies in the 21st century (Nord et al., 2019). IoT technology consists of various interconnected devices, sensors, and systems that permit the control and monitoring of our surroundings, providing an extremely versatile tool that allows interaction with our environment in unprecedented ways. Frost & Sullivan (2023) predicts active IoT-connected devices will reach 41.76 billion in 2023, up 18% from 2022. The acceleration of automation processes is driving this growth, companies' continued digital transformation journey, the recovery of value chains after the economic impacts of the pandemic, and the rollout of 5G connectivity networks (Frost & Sullivan, 2023). Many scholars agree that privacy and security are essential for the successful deployment of IoT devices (e.g., Ransbotham et al., 2016; Sicari et al., 2016; Fernandes et al., 2017; Koo & Kim, 2017; Heer et al., 2011). The U.S. Department of Homeland Security (DHS) published a report in 2014 (DHS, 2014) that identified several vulnerabilities in the IoT ecosystem. Attackers could exploit these vulnerabilities to access IoT devices and networks, potentially leading to data breaches, service disruptions, or physical damage.

The vast amounts of data collected and transmitted by IoT devices may be utilized to exploit privacy and security weaknesses (Obaidat et al., 2020; Algarni et al., 2021). With the advancement of IoT technology, privacy and security concerns must be addressed to ensure data are kept safe from malicious actors (Bastos et al., 2018). Concerns about IoT privacy and security may impact users' willingness to use IoT technology (Koohang et al., 2022). This study aims to examine IoT privacy and security concerns among employees

within various organizations paying attention to several variables, i.e., job level, daily use of IoT, daily time spent using IoT, age, and gender. In line with the purpose of the study, we ask the following research question:

RQ1: *Are there significant mean differences between the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) and the dependent variable of IoT privacy concerns?*

RQ2*: Are there significant mean differences between the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) and the dependent variable of IoT security concerns?*

Review of the Literature

Burrus (2014) believed IoT is the most significant technology trend of our time. It is disrupting and transforming industries across the globe, and it is poised to create even more opportunities in the years to come. There are many definitions for IoT. For example, Ben-Daya, Hassini, and Bahroun (2019, p. 4721) described it as "… a network of physical objects that are digitally connected to sense, monitor, and interact within a company and between the company and its supply chain enabling agility, visibility, tracking, and information sharing to facilitate timely planning, control, and coordination of the supply chain processes." Huang et al. (2016, p. 5) defined it as "a worldwide network of physical objects using the Internet as a communication media." Koohang et al. (2022) explained that the IoT is a network of connected devices that collect and share data. These devices can be anything from smartphones and laptops to wearables and industrial machines. When connected, these devices can create a robust network that can be used to improve efficiency, productivity, and safety.

IoT privacy and security concerns

One of the foremost challenges of IoT systems revolves around the potential for privacy breaches (Paul, 2019). The massive volume of data collected and transmitted by IoT devices can be inadvertently leaked without users' awareness (Alshohoumi et al., 2019; Obaidat et al., 2020). Most IoT users have seen their activity used for unintended consequences, such as in retail, where buying behavior is sold to advertisers (Cichy et al., 2021). Privacy concerns extend beyond personally initiated activity to encompass crowd-sensing and data-aggregating technologies that monetize users' behavior and information (Baldini et al., 2018). The emergence of artificial intelligence and advanced technologies that gather public data, including device locations during the COVID-19 pandemic, has heightened public awareness regarding privacy issues surrounding IoT. In a large-scale survey in Britain, the perceived value of IoT was significantly influenced by privacy concerns (El-Haddadeh et al., 2019). Of course, user activity cannot be completely anonymous because networks need to authenticate access (Wang et al., 2020), elevating privacy concerns as a perennial issue.

The IoT industry continues to grapple with identifying untrusted devices, a security vulnerability (Algarni et al., 2021; Alghofaili & Rassam, 2022). Common security concerns when using IoT include weak authentication, vulnerable software, and inadequate encryption (Bharati & Podder, 2022). IoT needs better authentication setups, such as default usernames and passwords, which hackers can easily guess or exploit. The FBI has issued warnings regarding the prevalence of outdated or unpatched firmware in many IoT devices, which can contain known vulnerabilities that cybercriminals can exploit (Teller Vision, 2017). IoT devices often transmit data over unencrypted channels, which attackers can intercept and read. Designing highly secure IoT systems is a massive challenge for devices and users with less-than-optimal cyber hygiene combined with the growing sophistication of hackers (Ghaleb & Azzedin, 2021).

Given the literature on difficulties addressing privacy and security risks, users' IoT privacy and security concerns seem reasonable. The literature has limited information about whether these concerns are uniform across the population, and our little evidence is mixed. Some evidence indicates that IoT risk concerns are similar across age groups, from 30-year-olds up to 79-year-olds (Fristedt et al., 2021). In a study of 2,033 individuals in the UK, risk beliefs were generally neutral to high risk, with the higher risk ratings more common in older users (Cannizzaro et al., 2020). Lim (2010) found that age-related technology views correlated to the user's generation (when first learning about digital products). No studies have addressed how job level and employee use of IoT impact IoT privacy or security concerns. One study found that better-educated participants, perhaps more likely to be in upper-level jobs, had higher IoT risk perceptions (Zhu, 2019). Pew Research (2018) found that men were more concerned about device security than women.

In addition to individual variables, organizational culture can impact user experience with IoT devices. In a recent study, organizational culture affected user compliance with security policies (Nord et al., 2022). Managers and co-workers influence each other (Bulgurcu et al., 2010), so levels of IoT concern may adjust based on colleagues' views, with those exposed to more IoT activity focusing more on conversations around IoT concerns. If the employee's role makes them feel responsible for securing information, they may have deeper concerns and higher risk perceptions than others (Shadbad & Biros, 2021). Employees with a broader span of authority may have more access to IoT security policies, potentially increasing awareness and concerns (Koohang et al., 2022). Given this limited research, it is unclear how job level, frequency of IoT use, age, and gender will impact IoT concerns.

Methodology

Instrument

We chose two constructs from a study conducted by Sargent et al. (2023). The constructs are IoT privacy concerns and IoT security concerns. The IoT privacy concerns "defined as users' concerns about IoT service providers collecting personal information, using stored personal information for their advantage/profit, selling stored personal information in their databases to other companies, sharing stored personal information with other companies without users' authorization, and the stored personal information is unprotected from unauthorized access." The IoT security concerns are "defined as users' concerns about IoT botnets, IoT-based data breaches, IoT direct exploitation via various devices, IoT device hijacking, rogue IoT devices, lack of regular patches and updates, and IoT insecure interfaces." (Sargent et al., 2023). The constructs with their associated items are as follows:

IoT Privacy Concerns

1. I am concerned that IoT service providers are collecting personal information about me.
2. I am concerned that IoT service providers would use my stored personal information for their advantage/profit.
3. I am concerned that IoT service providers would sell my stored personal information in their databases to other companies.
4. I am concerned that IoT service providers would share my stored personal information in their databases with other companies without my authorization.
5. I am concerned that IoT service providers' databases containing my personal information are unprotected from unauthorized access.

IoT Security Concerns

1. I am concerned about the IoT botnet (i.e., a network of devices connected to the IoT, typically routers, that have been infected by malware) attempting to gain unauthorized access to user accounts on my IoT devices.
2. I am concerned about IoT-based data breaches, i.e., exploiting Internet-connected cameras and/or users' cloud services, allowing attackers access to potentially sensitive data or other valuable information.
3. I am concerned about direct exploitation via printers and other IoT devices I use that are a common access point for attackers to gain access to sensitive and confidential information.
4. I am concerned about the IoT devices "hijacking" that the attacker demands a ransom fee for the decryption key unlocking the files.
5. I am concerned about the rogue IoT devices (i.e., counterfeit malicious IoT devices) installed in secured networks without authorization.
6. I am concerned about the lack of regular patches and updates to my IoT devices.
7. I am concerned that my IoT devices have insecure interfaces.

The instrument used a seven-point Likert scale, i.e., 7 = Completely Agree, 6 = Mostly Agree, 5 = Somewhat Agree, 4 = Neither Agree nor Disagree, 3 = Somewhat Disagree, 2 = Mostly Disagree, and 1 = Completely Disagree.

Subjects & Procedure

Upon approval from the Institutional Research Board (IRB), the instrument was administered electronically by a professional Internet survey company to approximately 200 employees in the USA. At the time of this study, we received 141 completed surveys. We conducted an outlier test to eliminate the outliers in the dataset. This resulted in 138 final completed surveys for this study.

The participants were Male (N=68) and female (N=70) with various age groups, i.e., 18-29 years old (N=23), 30-44 years old (N=23), 45-60 years old (N=49), and above 60 years old (N=38). The participants were employed as C-level executives (N=18), senior management (N=14), middle management (N=39), intermediate (N=40), and entry-level (N=27). The participants were 18 years and older, and they were assured confidentiality and anonymity.

Data Analysis

Two separate univariate Analysis of Variances (ANOVA) procedures via IBM SPSS statistics version 28 were conducted to answer the research questions. For each procedure, there were multiple independent variables and one dependent variable. According to Mertler and Vannatta (2016), several requirements for the dataset must be met before running the univariate ANOVA, i.e., dependent variables must be continuous, each independent variable must have two or more levels, outliers must be eliminated, and a test of homogeneity of variances using Levene's test (a non-significant value suggests homogeneity of variance) must be conducted to determine the equality of variances of the dataset. A non-significant value from Levene's test indicates homogeneity of variance. The F value is calculated for each independent variable to see whether the significance of the groups on the dependent variable. For any significant results for groups of more than two levels, post hoc analysis is conducted. Finally, descriptive analyses show the means and standard deviation of the dependent variable with each independent variable.

Results

IoT Privacy Concerns

RQ1*: Are there significant mean differences between the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) and the dependent variable of IoT privacy concerns?*

Table 1 shows the results of the univariate ANOVA for the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) and the dependent variable of IoT privacy concerns. Within the dataset, the dependent variable (IoT privacy concerns) was continuous; all the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) had two or more levels. There was no relationship between the observations in each group or between the groups, and the outliers (N=3) were identified and eliminated. Finally, data were tested for homogeneity of variances using Levene's test, which determines the equality of variances of the data. The result of Levene's Test of Equality of Error was non-significant (p = .122), suggesting homogeneity of variance. As shown in Table 1, there were significant mean differences between the independent variables of job level, daily use of IoT, age, and the dependent variable (IoT privacy concerns). Table 2 shows the descriptives.

Job level: C-level executives had significantly greater IoT privacy concerns, and entry-level employees had the least IoT privacy concerns. The results of Post hoc analysis for job level reveal that the C-level executive group was statistically significant with the middle management group (p=.033) and the entry-level group (p=.001).

*Daily Use****:*** Users with extremely likely daily use of IoT had significantly greater IoT privacy concerns, and those with slightly likely daily use of IoT had the least privacy concerns. Post hoc analysis shows that the extremely likely daily use of the IoT group was statistically significant, with slightly likely daily use of the IoT group (p=.032).

Age: Older subjects had significantly higher IoT privacy concerns, and younger subjects had the least IoT privacy concerns. Post hoc analysis for age reveals that the 18-29 age group is statistically significant with the above 60 age group (p=.050).

Table 1: Univariate ANOVA - Tests of Between-Subjects Effects

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	52.352	14	3.739	3.255	<.001
Intercept	1956.287	1	1956.287	1702.606	**<.001**
Job Level	11.716	4	2.929	2.549	**.043**
Daily Use of IoT	17.296	3	5.765	5.018	**.003**
Daily Time Spent Using IoT	4.057	3	1.352	1.177	.321
Age	11.614	3	3.871	3.369	**.021**
Gender	2.965	1	2.965	2.581	.111
Error	141.326	123	1.149		
Total	4734.480	138			
Corrected Total	193.679	137			

Note: Dependent Variable: IoT Privacy Concerns

Table 2: Descriptives

IoT Privacy Concerns * Job Level			
Job Level	**Mean**	**N**	**Std. Deviation**
Executive / C-Level	6.6222	18	.60542
Senior Management	5.6571	14	1.58925
Middle management	5.6154	39	1.18622
Intermediate	5.8600	40	1.00174
Entry Level	5.1778	27	1.21191
Total	5.7362	138	1.18900
IoT Privacy Concerns * Daily Use of IoT			
Likely Daily Use of IoT	**Mean**	**N**	**Std. Deviation**
Extremely likely	5.9860	43	.96550
Very likely	5.7611	36	1.07949
Moderately likely	5.8182	33	1.11620
Slightly likely	5.1846	26	1.58788
Total	5.7362	138	1.18900
IoT Privacy Concerns * Daily Time Spent Using IoT			
Daily Time Spent Using IoT	**Mean**	**N**	**Std. Deviation**
1–2 hours	5.7182	44	1.13492
3–4 hours	5.8136	59	1.15003
5–7 hours	5.7565	23	1.08033
Over 7 hours	5.3833	12	1.75905
Total	5.7362	138	1.18900
IoT Privacy Concerns * Age			
Age	**Mean**	**N**	**Std. Deviation**
18-29	5.4087	23	1.16694
30-44	5.6071	28	1.09745
45-60	5.6000	49	1.13652
Above 60	6.2053	38	1.24117
Total	5.7362	138	1.18900
IoT Privacy Concerns * Gender			
Gender	**Mean**	**N**	**Std. Deviation**
Male	5.5971	68	1.24229
Female	5.8714	70	1.12728
Total	5.7362	138	1.18900

IoT Security Concerns

RQ2: *Are there significant mean differences between the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) and the dependent variable of IoT security concerns?*

Table 3 shows the results of the univariate ANOVA for the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) and the dependent variable of IoT privacy concerns. Within the dataset, the dependent variable (IoT privacy concerns) was continuous; all the independent variables (job level, daily use of IoT, daily time spent using IoT, age, and gender) had two or more levels. There was no relationship between the observations in each group or between the groups, and the outliers

(N=3) were identified and eliminated. Finally, data were tested for homogeneity of variances using Levene's test, which determines the equality of variances of the data. The result of Levene's Test of Equality of Error was non-significant (p = .394), suggesting homogeneity of variance. Table 3 shows significant mean differences between the independent variables of job level and daily use of IoT and the dependent variable (IoT security concerns). Table 4 includes the descriptives.

Job level: C-level executives had significantly greater IoT privacy concerns, and entry-level employees had the least IoT privacy concerns. Post hoc analysis for job level and IoT security concerns reveals that the C-level executive group was statistically significant with the entry-level group (p=.003).

Daily Use: Users with extremely likely daily use of IoT had slightly higher IoT privacy concerns, and users with slightly likely daily use of IoT had the least IoT privacy concerns. However, Post hoc analysis showed that no groups were statistically significant compared to other groups.

Table 3: Univariate ANOVA - Tests of Between Subjects Effects

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	39.599	14	2.829	2.517	.003
Intercept	1752.278	1	1752.278	1559.382	<.001
Job Level	10.962	4	2.740	2.439	**.050**
Daily Use of IoT	13.877	3	4.626	4.117	**.008**
Daily Time Spent Using IoT	3.066	3	1.022	.910	.439
Age	7.525	3	2.508	2.232	.088
Gender	1.629	1	1.629	1.450	.231
Error	138.215	123	1.124		
Total	4218.265	138			
Corrected Total	177.814	137			

Note: Dependent variable: IoT security concerns

Table 4: Descriptives

IoT Security Concerns * Job Level			
IoT Security Concerns			
Job Level	**Mean**	**N**	**Std. Deviation**
Executive / C-Level	6.2619	18	.80253
Senior Management	5.1224	14	1.65545
Middle management	5.4762	39	1.10770
Intermediate	5.3821	40	.89208
Entry Level	4.9418	27	1.13061
Total	5.4110	138	1.13926
IoT Security Concerns * Daily Use of IoT			
Likely Daily Use of IoT	**Mean**	**N**	**Std. Deviation**
Extremely likely	5.6777	43	.92166
Very likely	5.2778	36	1.16506
Moderately likely	5.5455	33	.95595
Slightly likely	4.9835	26	1.50120
Total	5.4110	138	1.13926

Table 4: Descriptives (Cont.)

IoT Security Concerns * Daily Time Spent Using IoT			
Daily Time Spent Using IoT	**Mean**	**N**	**Std. Deviation**
1–2 hours	5.4740	44	1.10733
3–4 hours	5.4431	59	1.12100
5–7 hours	5.3354	23	1.01163
Over 7 hours	5.1667	12	1.61260
Total	5.4110	138	1.13926
IoT Security Concerns * Age			
Age	**Mean**	**N**	**Std. Deviation**
18-29	5.2609	23	1.02261
30-44	5.2704	28	1.14572
45-60	5.2770	49	1.04059
Above 60	5.7782	38	1.27676
Total	5.4110	138	1.13926
IoT Security Concerns * Gender			
Gender	**Mean**	**N**	**Std. Deviation**
Male	5.3298	68	1.19300
Female	5.4898	70	1.08731
Total	5.4110	138	1.13926

Discussion

Theoretical implications

Our work contributes significantly to the literature by establishing how job level, age, and daily use of IoT significantly influence IoT privacy and security concerns. The evidence shows that higher job levels and daily IoT use significantly influence security concerns. This supports prior work showing that leaders (high job levels), and the culture they create around technology, impact IoT trust (Nord et al., 2019). Our findings also indicate that those using IoT frequently have heightened security concerns, perhaps because they are more exposed to security policies and threats or colleagues that discuss these issues (Bulgurcu et al., 2010). This supports the literature that IoT awareness leads to security concerns (Koohang et al., 2022).

This study reports that privacy concerns were more likely for older users, those at higher job levels, and more frequent IoT users. This is the first work to report that job level leads to IoT privacy and IoT security concerns. The findings are consistent with studies examining job roles and trust in IoT (Hong & Xu, 2021; Shadbad & Biros, 2021). This new independent variable, job level, and how it impacts IoT privacy and security concerns opens rich opportunities for organizations to learn how job level informs privacy and security concerns. For instance, a recent study connected job roles with higher security policy compliance (Nord et al., 2022). Future work focused on job level and related higher privacy and security concerns could lead to understanding whether elevated concerns reflect greater awareness about IoT risks, doubt about the IoT strategy defending effectively against those risks, or both. The finding that older users have more privacy concerns contradicts work that shows IoT concerns are similar across age groups (Fristedt et al., 2021) and supports work that indicates that older users are less confident and have more significant concerns than younger users (Hua et al., 2020; Jang & Yu, 2017; Zhu, 2019).

Practical implications

Successful deployment of IoT requires addressing security and privacy concerns (Ransbotham et al., 2016; Sicari et al., 2016; Fernandes et al., 2017; Koo & Kim, 2017; Heer et al., 2011). The evidence in this project indicates that we need to address the higher security and privacy concerns for older users, those in higher-level jobs, and more frequent IoT users. Organizations can educate employees on essential tasks that improve privacy, especially for older and frequent IoT users, such as activating privacy settings, strengthening passwords, and adding multi-factor authentication (Tawalbeh et al., 2020). In addition, employers can share best practices for measuring device trust scores and identifying malicious nodes (Bi et al., 2023; Dhelim et al., 2023), demonstrating how they defend against privacy threats and directly address user privacy concerns.

For security concerns, a high-quality IoT security policy and trust management system, with leadership that cultivates robust security compliance, is an essential first step (Nord et al., 2022). Cybercriminals know how to exploit the weakest link in the security system, the employees (Chen et al., 2021), so IoT security training may help reduce user concerns and organizational security risks. Research indicates that the more you know about IoT risks, the more IoT concerns you have. Unfortunately, IoT security is a complex technical area prone to failures (Alghofaili & Rassam, 2022), so concerns are likely well-founded, especially for heavy users and those with a broader span of responsibility. Uniform security standards for devices, such as those proposed by IoT Security Foundation (2021), may help improve IoT security. A comprehensive IoT strategy would include privacy and security mitigation practices, such as next-generation firewalls and penetration testing may strengthen security (Sargent, 2023).

Research might investigate whether skillful leaders use higher awareness and concerns to boost the importance of compliance with security policies. Further, future studies could track education efforts to investigate if better-informed users have fewer IoT privacy and security concerns. While we did not collect data on industry-specific devices, this is a possible extension of our work. The medical Internet of Things (M-IoT) has gained a lot of attention in recent years and is a rapidly growing field with the potential to revolutionize healthcare. M-IoT has been described as "a group of devices connected to the Internet to perform the processes and services that support healthcare" (Sun et al., 2019, p. 1). Given the importance of M-IoT, future research might focus on whether employees using M-IoT devices to collect and transmit sensitive patient health data in real-time have heightened concerns about privacy and security.

Conclusion

This study investigated whether demographics (gender and age), job level, frequency of IoT use, and hours per day on IoT tasks of employees were related to IoT privacy and security concerns. Results indicated that older workers in higher job levels and more frequent IoT users have significantly deeper IoT privacy concerns. Further, higher job levels and frequency of IoT use significantly influenced employees' security concerns.

This work highlights that not all employees have the same privacy and security concerns. Knowing that user demographics, jobs, and frequency of IoT use influence IoT privacy and IoT security concerns helps organizations know to spend more time educating older, more frequent, and those in high-level jobs about IoT privacy and IoT security issues. Given the sparse evidence in the literature about how IoT users differ in their level of concern about privacy and security, more research is needed to understand these differences so organizations can address these critical concerns.

References

Algarni, M., Alkhelaiwi, M., & Karrar, A. (2021). Internet of Things Security: A Review of Enabled Application Challenges and Solutions. *International Journal of Advanced Computer Science and Applications, 12*(3). https://doi.org/10.14569/IJACSA.2021.0120325

Alghofaili, Y., & Rassam, M. A. (2022). A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. *Sensors* (14248220), *22*(2), 634–N.PAG. https://doi.org/10.3390/s22020634

Alshohoumi, F., Sarrab, M., AlHamadani, A., & Al-Abri, D. (2019). Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns. *International Journal of Advanced Computer Science and Applications, 10*(7). https://doi.org/10.14569/IJACSA.2019.0100733

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical design in the Internet of Things. *Science and engineering ethics*, *24*, 905-925.

Bastos, D., Shackleton, M., & El-Moussa, F. (2018). *Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments*. The Institution of Engineering & Technology. https://doi.org/10.1049/cp.2018.0030

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: A literature review. *International Journal of Production Research*, *57*(15–16), 4719–4742.

Bharati, S., & Podder, P. (2022). Machine and deep learning for IoT security and privacy: applications, challenges, and future directions. *Security and Communication Networks*, *2022*, 1-41. https://doi.org/10.1155/2022/8951961

Bi, L., Muazu, T., & Samuel, O. (2022). IoT: A Decentralized Trust Management System Using Blockchain-Empowered Federated Learning. *Sustainability*, *15*(1), 374. https://doi.org/10.3390/su15010374

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-A7. https://doi.org/10.2307/25750690

Burrus, D. (2014). The Internet of Things is Far Bigger than Anyone Realizes. Retrieved May 05, 2023 from https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/.

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS ONE*, *15*(5), 1–30. https://doi.org/10.1371/journal.pone.0231615

Chen, Q., Yuan, Y., Feng, Y., & Archer, N. (2021). A decision paradox: benefit vs risk and trust vs distrust for online dating adoption vs non-adoption. *Internet Research*, *31*(1), 341–375. https://doi.org/10.1108/INTR-07-2019-0304

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. *MIS Quarterly*, *45*(4), 1863–1891. https://doi.org/10.25300/MISQ/2021/14165

Dhelim, S., Aung, N., Ning, H., Chen, L., & Lakas, A. (2023). Trust2Vec: Large-Scale IoT Trust Management System based on Signed Network Embeddings. *IEEE Internet of Things*, *10*(1), 1-10.

DHS (2014). *Strategic Principles for Securing the Internet of Things (IoT)*. Retrieved May 05 from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

El-Haddadeh, R., Weerakkody, V., Osmani, M., Thakker, D., & Kapoor, K. K. (2019). Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement. *Government Information Quarterly*, *36*(2), 310-320. https://doi.org/10.1016/j.giq.2018.09.009

Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2017). Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? *IEEE Security & Privacy, 15*(4), 79-84. https://doi.org/10.1109/MSP.2017.3151346

Fristedt, S., Svärdh, S., Löfqvist, C., Schmidt, S. M., & Iwarsson, S. (2021). Am I representative (of my age)? No, I'm not - Attitudes to technologies and technology development differ but unite individuals across rather than within generations. *PLoS ONE*, *16*(4), 1–19. https://doi.org/10.1371/journal.pone.0250425

Frost & Sullivan (2023). *The Top Growth Opportunities for IoT in 2023*. Retrieved May 05 from https://www.frost.com/

Ghaleb, M., & Azzedin, F. (2021). Towards scalable and efficient architecture for modeling trust in IoT environments. *Sensors*, *21*(9), 2986.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications, 61*(3), 527-542, https://doi.org/10.1007/s11277-011-0385-5.

Hong, Y. and Xu, M. (2021). Autonomous motivation and information security policy compliance: role of job satisfaction, responsibility, and deterrence. *Journal of Organization and End User Computing*, *33* (6): pp. 1-16. https://doi.org/10.1109/JIOT.2022.3201772

Hua, C., Cole, S., & Xu, N. (2021). Rethinking trust in tourism apps: the moderating effect of age. *Journal of Hospitality & Tourism Technology*, *12*(3), 548–562. https://doi.org/10.1108/JHTT-01-2020-0013

Huang, X., Craig, P., Lin, H., & Yan, Z. (2016). SecIoT: A Security Framework for the Internet of Things. *Security and Communication Networks, 9*(16), 3083–3094.

IoT Security Foundation (2021). *IoT security assurance framework release 3.0*. Retrieved March 24, 2023, from https://www.iotsecurityfoundation.org/best-practice-guidelines/

Jang, S. & Yu, C. H. (2017). A Study on Internet of Things (IoT): Users' Reuse Intention Using Technology Acceptance Model in Korea. *International Journal of Business & Management Science*, *7*(2), 279–295.

Koo, C., & Kim, J. (2018). Enforcing high-level security policies for Internet of Things. *The Journal of Supercomputing*, *74*(9), 4497-4505. https://doi.org/10.1007/s11227-017-2201-9

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management, 62*(2). https://doi.org/10.1016/j.ijinfomgt.2021.102442

Lim, C. C. (2010). Designing inclusive ICT products for older users: taking into account the technology generation effect. *Journal of Engineering Design*, *21*(2/3), 189–206. https://doi.org/10.1080/09544820903317001

Mertler, C. A., & Vannatta, R. A. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation*. Taylor & Francis.

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, 97-108.

Nord, J. N., Sargent, C. S., Koohang, A. & Marotta, A. (2022). Predictors of success in information security policy compliance. *Journal of Computer Information Systems*, *62*(4), 863-873. https://doi.org/10.1080/08874417.2022.2067795

Obaidat, M. A., Obeidat, S., Holst, J., Hayajneh, A. A., & Brown, J. (2020). A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers, 9*(2), 44. https://doi.org/10.3390/computers9020044

Paul, F. (2019). IoT security vs. privacy: Which is a bigger issue?: When it comes to the internet of things (IoT), security has long been a key concern. But privacy issues could be an even bigger threat. *Network World (Online),* https://www.proquest.com/trade-journals/iot-security-vs-privacy-which-is-bigger-issue/docview/2239330843/se-2

Pew Research Center (2018). Americans' complicated feelings about social media in an era of privacy concerns. Retrieved February 20, 2023 from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special Section Introduction - Ubiquitous IT and Digital Vulnerabilities. *Information Systems Research,* 27(4), 834–847.

Sargent, C., Koohang, A. (2023). *Internet of Things (IoT) Risk beliefs: Influence on users' concerns about privacy, security, awareness, and device use*. Unpublished manuscript, Mercer University and Middle Georgia State University.

Shadbad, F., & Biros, D. (2021). Understanding Employee Information Security Policy Compliance from Role Theory Perspective. *Journal of Computer Information Systems*, *61*(6), 571–580. https://doi.org/10.1080/08874417.2020.1845584

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A Security-and Quality-Aware System Architecture for Internet of Things. *Information Systems Frontiers*, *18*(4), 665-677. https://doi.org/10.1007/s10796-014-9538-x.

Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access, 7*, 183339-183355. doi:10.1109/ACCESS.2019.2960617

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences, 10*(12), 4102. https://doi.org/10.3390/app10124102

Zhu, X. (2019). Segmenting the public's risk beliefs about drone delivery: A belief system approach. *Telematics & Informatics*, *40*, 27–40. https://doi.org/10.1016/j.tele.2019.05.007