Investigating Users' Privacy Concerns of Internet of Things (IoT) Smart Devices

Daniel Joy
Computer Science and Mathematics
Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA
danieljoy2345@gmail.com

Olivera Kotevska
Computer Science and Mathematics
Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA
kotevskao@ornl.gov

Eyhab Al-Masri
School of Engineering and Technology
University of Washington Tacoma
Tacoma, USA
ealmasri@uw.edu

***Abstract*—Although the number of smart Internet of Things (IoT) devices has grown in recent years, the public's perception of how effectively these devices secure IoT data has been questioned. Many IoT users do not have a good level of confidence in the security or privacy procedures implemented within IoT smart devices for protecting personal IoT data. Moreover, determining the level of confidence end users have in their smart devices is becoming a major challenge. In this paper, we present a study that focuses on identifying privacy concerns IoT end users have when using IoT smart devices. We investigated multiple smart devices and conducted a survey to identify users' privacy concerns. Furthermore, we identify five IoT privacy-preserving (IoTPP) control policies that we define and employ in comparing the privacy measures implemented by various popular smart devices. Results from our study show that the over 86% of participants are very or extremely concerned about the security and privacy of their personal data when using smart IoT devices such as Google Nest Hub or Amazon Alexa. In addition, our study shows that a significant number of IoT users may not be aware that their personal data is collected, stored or shared by IoT devices.**

Keywords—intelligent virtual assistants, privacy, security, personal data, IoT devices, smart devices, internet of things, differential privacy, privacy, data protection, security.

I. INTRODUCTION

In the past decade, the global smart device market has surged, creating a massive influx of user-generated data. By 2025, it is estimated that 41.6 billion Internet of Things (IoT) devices will be connected to the Internet, producing around 79.4 zettabytes of data [1]. The vast majority of this data will consist of video surveillance, audio, and images. Smart homes and hospitals are common locations for the deployment of the smart devices, therefore, the data generated by these devices is likely to contain sensitive and personal information. This raises some concerns as to whether IoT data needs to be full encrypted.

However, about 98% of IoT device traffic is not secured or encrypted and is transferred in the open over the Internet [2]. On average, IoT devices are probed for vulnerabilities in their security about 800 times per hour, with 400 login attempts and 130 successful logins on each device [3]. Therefore, IoT security is becoming an important challenge for developing, employing and maintaining IoT devices, particularly as the number of connected IoT devices and the amounts of IoT data continues to grow. More effective privacy and security algorithms are required to prevent malicious users from gaining access to sensitive or critical IoT users' data. Privacy algorithms are assisting in the protection of sensitive information for individuals while allowing many companies to undertake data analytics.

Differential Privacy (DP) [4] is used to preserve privacy on collected or generated data. It is a privacy-protection method that adds noise derived from the respective distributions. The added noise randomizes the data and eliminates individuality. hey demonstrated DP's effectiveness in protecting sensitive data generated by IoT devices. Existing research studies [5] show that many IoT devices collect sensitive information and share them with other platforms, while users are not well informed about this behavior. However, some work has been done in smart metering systems [6], for example, where DP was implemented on the edge IoT networks [7]. In this research paper, we investigate the use of differential privacy for smart IoT devices for privacy preservation.

There are many benefits of employing differential privacy for IoT data, but determining the level at which IoT data need to be analyzed as part of this process is a challenge since multiple criteria need to be considered. Multi-criteria decision making (MCDA) methods such as the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) [8] offer reliable mechanisms for improving the decisions for protecting the privacy of IoT users. TOPSIS, for example, has been successfully applied for resource allocation [9], and service provisioning across fog environments [10]. TOPSIS first determines the ideal best and ideal worst options. The Euclidean distance is used to determine an optimal solution among all possible options or alternatives. The option or alternative closest to the optimal best solution is the one that is recommended by this MCDA method.

In the case of differential privacy for IoT devices, TOPSIS can be employed to identify the appropriate levels or effectiveness of privacy protection policies when using IoT devices [11]. A criteria comprised of a number of privacy-related features or attributes can be used to measure such effectiveness. Because of the fact that IoT devices may constantly switch among various data types and can possess adding new features dynamically, methods such as TOPSIS can automatically recommend IoT devices or even sensors that can be employed for completing IoT tasks. Through TOPSIS, for example, it is then possible to optimize the resources required for completing IoT tasks while increasing the performance of IoT devices. To this extent, in this paper, we evaluated the use of the MCDA method TOPSIS while examining the impact of employing differential privacy on IoT data generated by IoT devices.

In this paper, we explore the vulnerabilities of smart home IoT devices and users' perception on IoT data privacy preservation. We conduct a survey on the plurality of IoT devices to determine this perception from end users' perspective. We also employ an implementation of differential privacy on IoT data and investigate its impact for decision making based on the TOPSIS MCDA method. Finally, we demonstrate the effectiveness of employing differential privacy on enhancing the privacy IoT users' data. The rest of this paper is organized as follows. Section II describes our proposed survey and methodology. Results and discussion are discussed in Section III. Finally, conclusion and future work are described in Section IV.

II. Methodology

We conducted a literature review to identify crucial or fundamental privacy-related characteristics that IoT applications or devices should or are likely to possess [12-24]. To this extent, a number of privacy-preserving features that IoT devices should possess or support in order to ensure a level of protection for IoT users' data throughout the various stages, including data collection, transmission, and sharing. Using a survey, we employ these IoTPP controls to determine the degree to which existing IoT users are aware of the extent to which IoT devices protect their personal data and preserve their privacy.

A. IoT Privacy-Preserving (IoTPP) Controls

We identify five IoT data privacy-preserving (IoTPP) controls or characteristics: authentication, authorization, anonymization, denaturation, and digital forgetting. These IoTPP controls are defined in the following subsections.

- Authentication: This privacy-preserving characteristic specifies the extent to which an IoT device is capable of correctly verifying the identity of an IoT end user.
- Authorization: This privacy-preserving attribute indicates the extent to which an IoT device can establish one or more network connections with other devices and/or exchange acquired data.
- Anonymization: This privacy-preserving attribute indicates the extent to which an IoT device can permanently remove or temporarily hide personally identifiable information from data acquired through IoT constructs (e.g., Sensors) existing on the IoT device.
- Denaturation: This privacy-preserving characteristic describes the extent to which an IoT device is capable of eliminating or modifying personally identifiable information from acquired IoT data (e.g., Blurring a face in a collected image or video).
- Denaturation: This privacy-preserving attribute describes the extent to which an IoT device is able to permanently delete or eliminate IoT data, either locally or remotely, or its traces after a specified period of time, after certain conditions have been met, or after an event has occurred (e.g., cancel subscription).

B. Privacy Policies

As a preliminary stage in the design of this study, we conducted research on a variety of existing IoT vendors, review platforms, and online electronic commerce portals to identify the most popular smart IoT devices in recent years. Then, we reviewed and examined the official technical documentation for IoT vendors to determine if they utilize any, some, or all of the aforementioned IoTPP characteristics. We manually examined the documentation provided by IoT vendors for each IoT device considered.

Based on the highest customer ratings, we evaluated eighteen popular smart IoT devices with a variety of functions (e.g., doorbell, camera, personal assistant, etc.). Then, we examine the IoT device application and/or official vendor documentation based on the IoTPP controls defined in Section A. A score was manually assigned to each IoTPP control policy on a scale from 1 to 5, where a low score indicates a high risk of data leakage (i.e., the least privacy-preserving) and a high score indicates a very low risk (e.g., most privacy-preserving). In addition to the manual score assignment, we developed a web scraping service that extract the IoTPP control policy information automatically based on keyword frequency. Then, scores were normalized and combined with that of the manually-assigned scores to generate the final IoTPP control policy scores for each device.

To illustrate how we used official technical documentation for determining IoTPP control policy scores. Consider for example an IoT device that processes the capturing of video calls, the IoT device or hub managing the communication may store such calls by a service provider. In such cases, an IoT hub or gateway may deploy a technique that blurs faces to preserve privacy of users when recording video calls. In this instance, the IoT device offers support for the IoTPP denaturing control and a score will be provided for that category.

Another example is to consider an IoT device that allows the controlling or issuing commands to other IoT devices (such as Amazon Alexa and Ring doorbell). In such case, the Ring doorbell device delegates the authorization to Amazon Alexa. Hence, a score is assigned for the authorization IoTPP control policy for that device.

An additional example is the use of digital forgetting which is supported by an IoT device for allowing end users to delete or remove any recorded data or activity logs. After the collection of this information, we developed multiple use cases to demonstrate how IoT devices may preserve the privacy of user data by implementing the five IoTPP control policies and characteristics. We further use this information to present to participants of a survey that we developed with specific examples in the form of an instructional guide to educate them on the significance of these controls.

We utilized the Technique for Order of Preference by Similarity to Ideal Solution, a multi-criteria decision making technique, because assigning a score manually involves an expert decision maker to provide IoTPP control policy scores (TOPSIS). TOPSIS compares a collection of inputs by evaluating their weights and calculating the geometric distance between each alternative and the optimal solution [25]. In our case, an IoT device represents an alternative, and the inputs or criteria are the five IoTPP control policies. In terms of data privacy, the TOPSIS score indicates the overall privacy-preserving score.

C. Developing the Survey: Collectiing Public Opinion

As part of study, we designed a questionnaire to assess the public's awareness or understanding of privacy concerns or challenges related to the collection of IoT data by IoT devices. The overarching objectives of the survey are to determine the

degree to which IoT users are aware that IoT devices may collect their personal data and to identify any privacy-related concerns IoT users may have when sharing or storing their personal data via IoT devices or IoT vendor services (e.g., via the cloud or edge gateways).

To this end, we invited responses from participants aged 18 and older for the survey that we developed. The survey was available online and was completely anonymous. We asked participants a series of questions divided across multiple sections.

In the first section of the survey, we provide participants with a brief explanation and illustrative examples of each of the IoTPP controls described in Section A. Then, we ask participants to provide opinion on five of the most popular smart IoT devices identified through other surveys [26], existing review platforms, and online retailers. These devices include: (a) Amazon Alexa, (b) Google Nest Hub, (c) Ring Doorbell Pro, (d) Sleep Number Smart Bed, and (e) Qardio SmartScale.

As part of the first section, we ask participants to identify, based on a scale ranging between 1-5 of their perception about the relationship of each IoTPP control to each of the five examined IoT devices where level 1 indicates no data privacy preservation is employed and level 5 indicates complete trust of the end user in the IoT device preserving the privacy of personal IoT data.

In contrast to the first section, which was device-specific, we asked participants in the second section of the survey general questions about their familiarity with or level of concern in terms of privacy-preservation of IoT data within smart IoT devices. In this respect, three questions were asked to participants:

- *Do you believe that people need to be tech-savvy to use smart devices?*
- *How concerned are you currently about data privacy and smart devices?*
- *With the previous information in mind, how do you now feel about data privacy and smart devices?*

In the third section, participants' general demographic information is collected. In this regard, we inquired about participants' age groups and geographic area (e.g., Midwest, Northeast, etc.).

During the survey's open time (06/27/2022 - 07/11/2022), we received a total of fifty-two responses. The age group of the participants is between 18 and 65 years. We use the data collected from this anonymous survey to conduct additional analysis and segmentation of the results, as described in Section III. We also discuss the results with respect to privacy concerns based on the data we collected from the survey. Finally, the conclusion and future work is provided in Section IV.

D. Differential Privacy (DP)

Differential Privacy (DP) enables the sharing of datasets in which patterns of groups within the dataset can be described while hiding or withholding data about individual entities [27-30]. Differential privacy can be achieved when the results of an analysis are identical regardless of whether or not a particular data point is included in a dataset [4, 29, 30]. An option for achieving this is to introduce random noise to each item in the dataset. For instance, adding Laplacian noise to a dataset and adjusting two parameters, sensitivity and epsilon (ϵ), are examples of controlling level of withholding data about individual entities [29]. The sensitivity parameter is determined by the difference in size between the original dataset and the dataset resulting from removing one item. The epsilon (ϵ) parameter is chosen based on much privacy loss is required by the user [27, 28].

In order to examine the use of differential privacy for preserving the privacy of IoT data, we developed a series of use cases involving sequence of possible events for using IoT devices. To this extent, we employed the Markov Process to describe such sequences of events. We considered the following sensors: motion sensor, light switch, and doorbell and security camera. We developed multiple use cases for employing these sensors reflecting some of the daily routines of utilizing these sensors within IoT devices in a typical smart home environment. The simulation output was formatted to be a list of size 1440 (the amount of minutes in a day). We used a state element to indicate whether a sensor is in an OFF (0) or ON (1) state, respectively. DP was then applied to this list of simulated events. The sensitivity and epsilon parameters were iterated through to find optimal values.

III. Results and Discussion

A. Experimental Setup

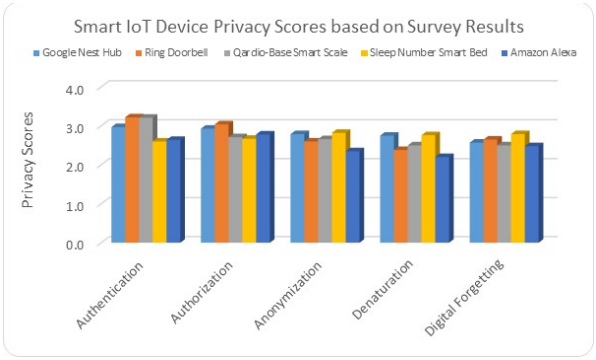
We implemented the experiments using the Python language (ver. 3.8) with the following libraries: sklearn, numpy, random, math and time for math and time, seaborne, nltk, and matplotlib. Most of the experiments were conducted using Google Colab, which has 20GB RAM and 70GB storage space. All experiments were repeated five times.

B. Using TOPSIS for Decision Making

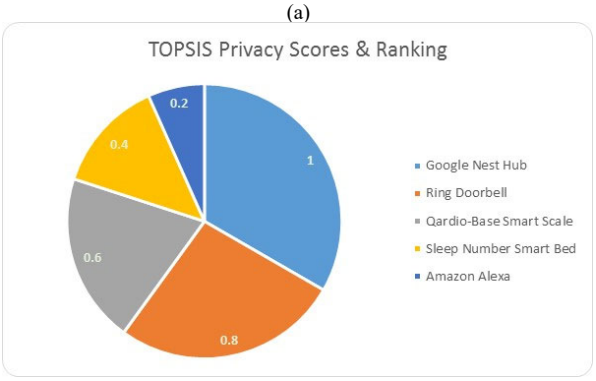
Based on the fifty two responses received from our survey, we computed the average value from the responses received to questions regarding data privacy attributes. We then used this data to design a decision matrix used as an input for the TOPSIS algorithm. We employed an equal weightage parameter across all IoTPP control policies. Results from the survey with respect to the privacy scores are shown in Figure 1.Using TOPSIS, we are able to employ multi-criteria decision making to achieve consistent and reliable ranking scores of IoTPP control policies. Additionally, TOPSIS supports our study in using the results from the survey to build an accurate decision matrix.

C. Privacy Scores Results

As shown in Figure 1, Google Nest Hub was rated the most trustworthy device in terms of data privacy, while Amazon Alexa was rated the least trustworthy. This indicates how well end users perceive these devices to protect their personal information. Seventy percent of the market share for voice assistants is dominated by Amazon Alexa (and/or Echo) according to a 2019 survey, while Google has approximately twenty-five percent [31]. Regarding IoTPP control policies, Google Nest Hub did not receive the highest scores across all. Respondents believe, for instance, that Ring Doorbell and Qardio-Base Smart scale have better privacy controls than Sleep Number Smart Bed, Google Nest Hub, and Amazon Alexa, respectively.



(a)



(b)

Fig. 1. (a) Smart IoT Device Privacy Scores based on Survey Results; (b) TOPSIS Ranking for Privacy Preservation

In addition, according to the perceptions of IoT end users regarding authentication, the Sleep Number Smart Bed is associated with the lowest score, with a small lead over Amazon Alexa. With a score of 2.78 out of 5 (or 55.6%) for privacy preservation in terms of authorization, many IoT end users believe Amazon Alexa is the worst among all of the five devices. With a rating of 3.04 out of 5 (60.8%), Ring Doorbell outranks other devices. For the anonymization control policy, the perception of Amazon Alexa among end users decreases to 47%. (or 2.35 out of 5). Amazon Alexa also receives the lowest rating (44.0%) for denaturation. Except for the Sleep Number Smart Bed, all devices score an average of 2.55 out of 5 (or 51%) for digital forgetting.

While the ranking in Figure 1 indicates that Google Nest has the highest rating and Amazon Alexa has the lowest, the results are intriguing when compared to the group averages. Many end-users do not believe that IoT devices are secure, capable of protecting their privacy, or preserve their privacy. Table 1 shows the average score for all IoTPP control policies.

As shown in Table 1, IoT end users have a very low level of trust in IoT devices protecting their personal data, averaging 2.70 out of 5 (or 54%). Authorization and authentication IoTPP control policies have marginally higher averages than denaturation. In addition, the collected scores exhibit some consistency with low standard deviation values and a score distribution centered on the median for each IoTPP control policy.

While some IoT devices may be ranked higher than others across the five IoTPP control policies, the survey results indicate a very low perceived quality in terms of IoT privacy and how IoT devices can protect their privacy when collecting, sharing, or storing data. In addition, 52.0% of IoT end users who participated in the survey believe that IoT devices offer the capacity to permanently delete or eliminate IoT data, either locally or remotely, as well as any traces over time. This result appears consistent with anonymization (53%) and denaturation (50%) outcomes.

D. IoTPP Control Policies and Data Types

Table 1 demonstrates a poor perception, perceived quality, or level of trust that end users have for IoT devices in terms of personal privacy preservation. In fact, none of the devices we examined has an average greater than three (or sixty percent), indicating that IoT end users have significant privacy concerns when using IoT devices to store or share personal data. The majority of respondents believe that IoT devices do not provide adequate levels of privacy protection for their personal data and that they do not provide guarantees of employing reliable or trustworthy techniques for removing or modifying personally identifiable information from IoT data.

TABLE I. IOTPP CONTROL POLICIY SCORING STATISTICS

	Average Score	Standard Deviation
Authentication	2.93	0.27
Authorization	2.83	0.14
Anonymization	2.64	0.17
Denaturation	2.52	0.22
Digital Forgetting	2.60	0.11
Average	2.70	

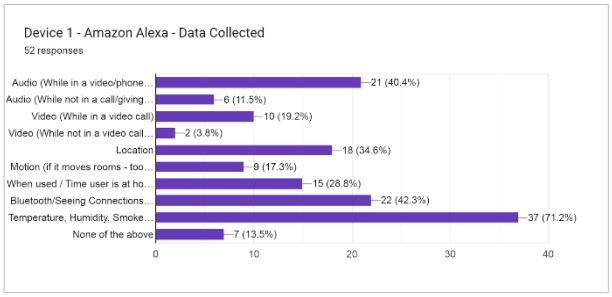
Since IoT devices may collect, store, or share various data types (e.g., audio, textual, or video), we asked participants, as part of the device-specific survey questionnaire, which data type, if any, they would be comfortable with the device collecting or storing? Participants may select multiple options from a list of possible options. Table II lists the potential responses to this question for two similar IoT devices.

TABLE II. DATA & DATA TYPES COLLECTION OPTIONS

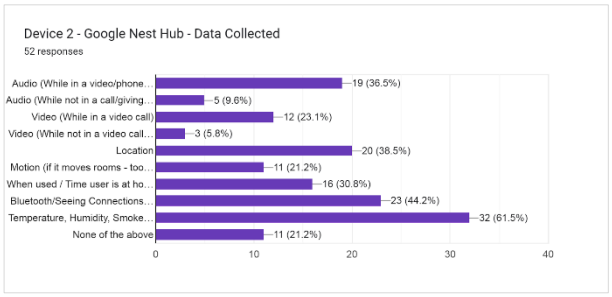
Audio (While in a video/phone call or using voice commands)
Audio (While not in a call/giving commands - passively collecting)
Video (While in a video call)
Video (While not in a video call - passively collecting)
Location
Motion (if it moves rooms - too precise for 'location' to detect)
When used / Time user is at home
Bluetooth/Seeing Connections to other Devices
Temperature, Humidity, Smoke levels

Google Nest Hub and Amazon Alexa, two known IoT devices that collect data, are compared in Figure 2. As shown in Figure 2, the majority of respondents are more comfortable with IoT devices collecting or storing textual data through sensors such as temperature, humidity, and smoke sensors than audio or video data collected or stored via microphones or cameras. This is true for both Amazon Alexa (71.2% of respondents) and Google Nest Hub (61% of respondents). In addition, end users are less comfortable with video data collection than audio data collection. In fact, the percentage of end users which are comfortable with Amazon Alexa capturing audio while they are on a phone call drops from 40.4% to 19.2%, for video recording. The same holds true for Google Nest Hub, which has a 36.5% audio capture rate compared to a 23.1% video capture rate.

Additionally, more than sixty percent of respondents did not feel comfortable with their location being collected (65.4% for Amazon Alexa and 61.2% for Google Nest Hub). Moreover, IoT end users become highly uncomfortable or insecure when IoT devices use motion sensors to track, record or monitor user locations or movements (e.g., between rooms in a smart home environment), with dissatisfaction rates of 82.7% and 78.8% for Amazon Alexa and Google Nest Hub, respectively.



(a)



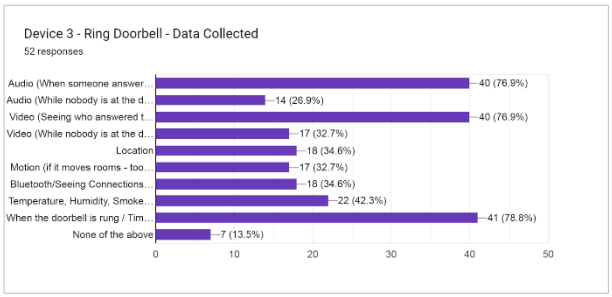
(b)

Fig. 2. Data Types Responses for (a) Amazon Alexa and (b) Google Nest Hub.

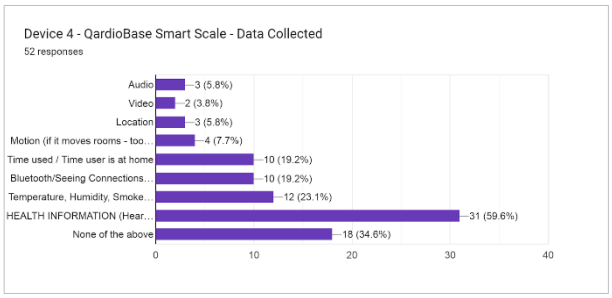
E. IoT End User's Familiarity with Privacy Concerns

Moreover, 96.2% and 94.2% of respondents do not feel at all comfortable with Amazon Alexa and Google Nest Hub collecting video data while end users are not on video calls (e.g., devices are in silent mode). The same holds true for audio captured off-device, although with relatively lower dissatisfaction rates for both devices. Overall, Figure 2 demonstrates that IoT end users do not trust IoT devices when capturing audio and video data and have significant privacy concerns concerning how such data is collected, stored, and shared over the Internet.

As shown in Figure 3, the respondents' confidence in the Ring Doorbell IoT devices' ability to collect auditory and visual data increases significantly by 76.9%. Compared to Amazon Alexa and Google Nest Hub, this level of comfort is nearly double for auditory data collection and four times greater for visual data collection. This indicates that IoT end users are more comfortable with the collection of auditory or visual data outdoors as opposed to indoors. This result also indicates that users have much less confidence in IoT devices protecting their privacy indoors than outdoors when it comes to the collection, recording or sharing of audio or video data containing personal information. Moreover, end users are much more comfortable with outdoor audio or video data recordings that can be tailored for protecting or safeguarding (e.g., homes) and are more willing to share personal information when required (e.g., trade-off of protection versus privacy).



(a)



(b)

Fig. 3. Data Types Responses for (a) QardioBase Smart Scale and (b) QardioBase Smart Scale.

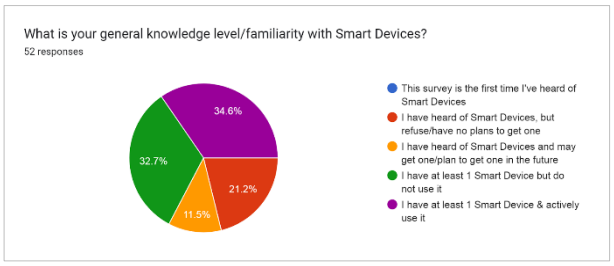
Figure 3 also demonstrates that the QardioBase Smart Scale has the lowest end-user confidence levels for audio and video data types, with dissatisfaction or uncertainty rates of 94.2% and 96.6%, respectively. Despite this, 59.6% of respondents are comfortable with textual health information.

While the extent to which IoT end users feel comfortable sharing auditory, textual, and visual data collections varies across the various IoT devices we examined or surveyed, it remains a fact that many users feel extremely uncomfortable sharing indoor location information that can be used to identify locations or movements. This outcome is conveyed by the results for Amazon Alexa, Google Nest Hun, and the QardioBase Smart Scale smart devices. The IoT device that appears to have the highest proportion of respondents who are comfortable with data sharing is the Ring Doorbell, which is generally designed to collect data outdoors and report it indoors through an IoT application (e.g., mobile app).

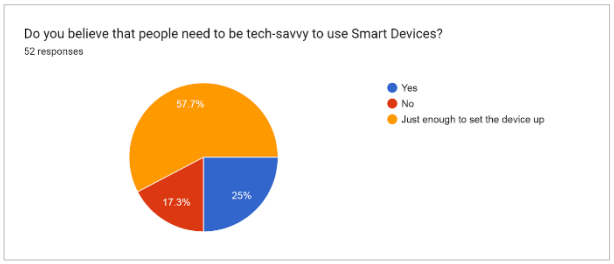
The responses to the familiarity questions regarding IoT devices are presented in Figure 4. Thirty-five respondents (or 67.30%) have at least one smart device, and 34.6% of those actively use it. These results are consistent with other studies that examined the average number of IoT devices owned or used by households. According to a recent study conducted by the Consumer Technology Association (CTA), nearly 70% of U.S. households own or use some form of smart home technology [32]. In addition, eleven respondents (or 34.6%) are aware of smart devices but have no intention or interest of acquiring or using them. Six respondents (or 11.5%) may acquire a smart device in the future.

In addition, Figure 4 demonstrates that 57.3% of respondents believe that end users do not necessarily need to be tech-savvy in order to set up smart devices. In fact, 25% of respondents (or 13 respondents) believe that being a tech savvy is not required to use smart devices. Figure 4 also demonstrates the prevalence of smart devices and the minimal technical expertise required for operating, installing, or utilizing IoT devices. In addition, Figure 4 demonstrates that the level of user-friendliness when employing smart devices or the intuitive interfaces they provide is acceptable,

reflecting the ease with which end users with little or no technical knowledge can interact with these devices.



(a)

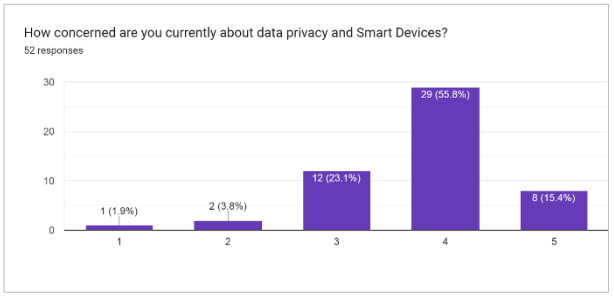


(b)

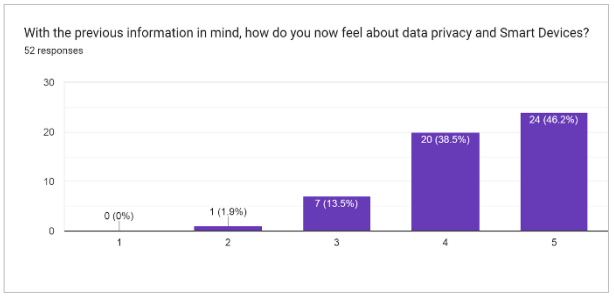
Fig. 4. Familiarity Questions from the Survey: (a) general knowledge question; (b) question about being tech-savvy for using IoT devices.

F. End User Privacy Concern Levels and Awareness

Figure 5 shows the responses of our survey respondents to questions regarding their current level of concern regarding data privacy when using smart devices. One of the questions relates to current privacy concerns (left), while the other relates to privacy concerns after reviewing earlier survey questions and learning more about privacy protection for smart IoT devices (right). On a scale from 1 to 5 (1 being least concerned and 5 being extremely concerned), the average rate of general concern is 3.78 out of 5 (or 75.6%). After end users are made aware of the IoTPP control policies and their implications, the average level of concern increases to 4.29 (85.8%). In such case, the awareness of privacy protection has increased end-users' concerns by 10.2%.



(a)



(b)

Fig. 5. Responses to a (a) a General Privacy Concerns Question; (b): Privacy Concerns Question after Learning about IoTPP Control Policies

More than eighty-six percent of respondents have serious privacy concerns, as shown by the distribution of responses between ratings of 4 (very concerned) and 5 (extremely concerned). In fact, awareness of the information provided in the survey has increased the number of respondents who are very concerned or extremely concerned from 71.2% to 86%, respectively. This increase demonstrates how critical it is for smart device users to be aware of privacy concerns. In addition, results show in Figure 5 demonstrate that the majority of IoT end users are very or extremely concerned about the security of their personal data when utilizing smart IoT devices.

G. Distribution of Privacy Policies in Documentation

We examined the official technical documentation for eleven smart devices to determine the extent to which such product documentation mention or discuss privacy-related policies such as authentication, authorization, encryption and deletion (representing Denaturation and digital forgetting together). The frequency distribution for the privacy policies we examined in the official documentation of smart devices investigated is shown in Figure 6.

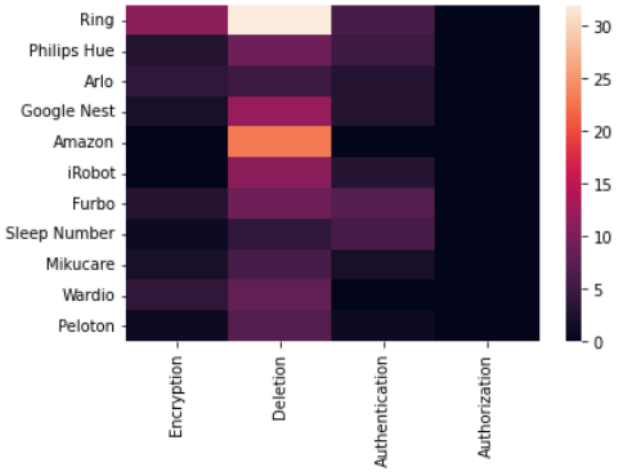


Fig. 6. Heat-Map of Word Count for IoT Privacy Attributes using web scraping. Legend: Light colors reflects high word frequency count whereas dark colors represent low word frequency count.

As shown in Figure 6, the Deletion category has the highest word frequency count compared to other categories. We observed that none of the devices' documentation mention the keywords “differential privacy” or “preserve” phrases. From the list of smart devices in Figure 6, we selected five devices to examine manually. These devices are the same set of devices used for the survey.

IV. Conclusion

In this paper, we presented the results from a survey study that examined the common IoT privacy-preserving (IoTPP) control policies across one or more smart IoT devices. Results from our survey show that 86% of IoT end users are very or extremely concerned about the privacy preservation techniques employed by existing IoT devices to protect their personal data. In addition, results from our survey show that more than 67% of participants currently own or use smart IoT devices.

Furthermore, we identify that the majority of IoT end users are more concerned about audio and video data type recordings compared to textual data collected. In addition, the plurality of IoT end users that we surveyed are concerned about the use of location or motion sensors that can be

employed for tracking or logging activities. Throughout the paper, we also provide some comparisons across some popular smart IoT devices such as Google Nest Hub, Ring Doorbell and Amazon Alexa. For future work, we plan to extend this study to determine the impact of privacy concerns prior and after using differential privacy.

REFERENCES

[1] The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast (2019), 2019, [online] Available: https://www.telecomtv.com/content/iot/the-growth-in-connected-iot-devices-is-expected-to-generate-79-4zb-of-data-in-2025-according-to-a-new-idc-forecast-35522. Last Accessed Nov 1, 2022.

[2] 2020 Unit 42 IoT Threat Report (2020), [online] Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020. Last Accessed Nov 1, 2022.

[3] 4 ways cyber attackers may be hacking your IoT devices right now (2021), [online] Available: https://www.hologram.io/blog/4-ways-cyber-attackers-may-be-hacking-your-iot-devices-right-now. Last Accessed Nov 1, 2022.

[4] Dwork, C. (2006). Differential Privacy. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds) Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science, vol 4052. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11787006_1

[5] Story, P., Smullen, D., Yao, Y., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2021). Awareness, adoption, and misconceptions of web privacy tools. Proceedings on Privacy Enhancing Technologies, 2021(3), 308-333.

[6] Peralta-Peterson, M., & Kotevska, O. (2021, December). Effectiveness of Privacy Techniques in Smart Metering Systems. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 675-678). IEEE.

[7] Kotevska, O., Johnson, J., & Kusne, A. G. (2022, June). Analyzing Data Privacy for Edge Systems. In 2022 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 223-228). IEEE.

[8] Tzeng, G. H., & Huang, J. J. (2011). Multiple attribute decision making: methods and applications. CRC press.

[9] Mohamed, H., Al-Masri, E., Kotevska, O., & Souri, A. (2022). A Multi-Objective Approach for Optimizing Edge-Based Resource Allocation Using TOPSIS. Electronics, 11(18), 2888.

[10] Pathak, P., & Al-Masri, E. (2020, October). Using TOPSIS for enhancing service provisioning across Fog environments. In 2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE) (pp. 272-275). IEEE.

[11] Oltramari, A., Piraviperumal, D., Schaub, F., Wilson, S., Cherivirala, S., Norton, T. B., ... & Sadeh, N. (2018). PrivOnto: A semantic framework for the analysis of privacy policies. Semantic Web, 9(2), 185-203.

[12] Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. computers & security, 37, 111-123.

[13] Lefkovitz, N., & Boeckl, K. (2020). NIST Privacy Framework: An Overview.

[14] Papadamou, K., Charalambous, M., Papagiannis, P., Stroinea, I., Passas, N., Xenakis, C., & Sirivianos, M. (2020). IdeNtity verifiCatiOn with privacy-preservinG credeNtIals for anonymous access To Online services. [online] Available: https://incognito.socialcomputing.eu/wp-content/uploads/2021/03/INCOGNITO_D4.1_revised_final_v3.pdf. Last Accessed Nov 1, 2022.

[15] Subramanian, J. (2021). Key Concepts in Privacy Technologies. [online] Available: https://blogs.sap.com/2021/08/22/key-concepts-in-privacy-technologies/. Last Accessed Nov 1, 2022.

[16] Oracle FLEXCUBE Investor Servicing Privacy by Design User Guide (2018). [online] Available: https://docs.oracle.com/cd/E94389_02/html/Privacy_By_Design/PII_02.htm. Last Accessed Nov 1, 2022.

[17] Liu, L. (2009). Privacy and location anonymization in location-based services. SIGSPATIAL Special, 1(2), 15-22.

[18] Shinzaki, T., Morikawa, I., Yamaoka, Y., & Sakemi, Y. (2016). IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data. Fujitsu Sci. Tech. J, 52(4), 52-60.

[19] Ribeiro, S. L., & Nakamura, E. T. (2019, October). Privacy protection with pseudonymization and anonymization in a health IoT system: results from ocariot. In 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE) (pp. 904-908). IEEE.

[20] Kunz, I., Schneider, A., Banse, C., Weiss, K., & Binder, A. (2022, November). Poster: Patient Community--A Test Bed for Privacy Threat Analysis. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 3383-3385).

[21] Aguru, A. D., Babu, E. S., Nayak, S. R., Sethy, A., & Verma, A. (2022). Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation. Algorithms, 15(9), 309.

[22] Lachner, C., Rausch, T., & Dustdar, S. (2021, May). A privacy preserving system for AI-assisted video analytics. In 2021 IEEE 5th International Conference on Fog and Edge Computing (ICFEC) (pp. 74-78). IEEE.

[23] Yin, X. C., Liu, Z. G., Ndibanje, B., Nkenyereye, L., & Riazul Islam, S. M. (2019). An IoT-based anonymous function for security and privacy in healthcare sensor networks. Sensors, 19(14), 3146.

[24] Seliem, M., Elgazzar, K., & Khalil, K. (2018). Towards privacy preserving iot environments: a survey. Wireless Communications and Mobile Computing, 2018.

[25] Lai, Y. J., Liu, T. Y., & Hwang, C. L. (1994). Topsis for MODM. European journal of operational research, 76(3), 486-500.

[26] Woodall, M. (2021). The Most Popular Smart Home Devices 2022. [online]. Available: https://www.reviews.org/home-security/most-popular-smart-home-device-statistics. Last Accessed Nov 1, 2022.

[27] Mironov, I., Pandey, O., Reingold, O., & Vadhan, S. (2009, August). Computational differential privacy. In Annual International Cryptology Conference (pp. 126-142). Springer, Berlin, Heidelberg.

[28] Kasiviswanathan, S. P., Lee, H. K., Nissim, K., Raskhodnikova, S., & Smith, A. (2011). What can we learn privately?. SIAM Journal on Computing, 40(3), 793-826.

[29] Dwork, C., & Yekhanin, S. (2008, August). New efficient attacks on statistical disclosure control mechanisms. In Annual International Cryptology Conference (pp. 469-480). Springer, Berlin, Heidelberg.

[30] Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006, March). Calibrating noise to sensitivity in private data analysis. In Theory of cryptography conference (pp. 265-284). Springer, Berlin, Heidelberg.

[31] Smart Speakers Global Market Report 2022 (2022). [online] Available: https://www.thebusinessresearchcompany.com/report/smart-speakers-global-market-report. Last Accessed Nov 1, 2022.

[32] Comiskey, B. (2020). The Ringing Future of Smart Home Technology. [online] Available: https://www.cta.tech/Resources/i3-Magazine/i3-Issues/2020/January-February/The-Ringing-Future-of-Smart-Home-Technology. Last Accessed Nov 1, 2022.