International Journal of Computer Science and Informatics

Volume 4 | Issue 3 Article 7

February 2022

A Study on Privacy of IoT Devices among a Sample of Indians in the U.S- 2021

Sahana Prasad Dr
CHRIST, sahanaprasad.p@gmail.com

Sharanya Prasad Ms
Cisco Systems, sharanya36@gmail.com

Vijith Raghavendra
CHRIST, raghavendra.vijith@gmail.com

Srishma Sunku
sunku.srishma@gmail.com

Recommended Citation

Prasad, Sahana Dr; Prasad, Sharanya Ms; Raghavendra, Vijith; and Sunku, Srishma (2022) "A Study on Privacy of IoT Devices among a Sample of Indians in the U.S- 2021," *International Journal of Computer Science and Informatics*: Vol. 4: Iss. 3, Article 7.
DOI: 10.47893/IJCSI.2022.1198
Available at: https://www.interscience.in/ijcsi/vol4/iss3/7

A Study on Privacy of IoT Devices among a Sample of Indians in the U.S- 2021

Cover Page Footnote
Thanks to all respondents of our questionnaire

A Study on Privacy of IoT Devices among a Sample of Indians In the U.S- 2021

Dr. Sahana Prasad*[1], MS. Sharanya Prasad [2], Vijith Raghavendra[1], Srishma Sunku[1]

[1]Christ (Deemed to be University), Bangalore, India

[2]CISCO Systems

Abstract

The Internet of Things (IoT) is the trendy and prominent term in the recent times with its wide-ranging applications in domains of medicine, science, military as well as domestic use. Despite its tremendous growth, privacy concerns plague IoT applications and have the potential to hamper the benefits derived from their usage. This paper carries out a statistical analysis of empirical data collected from users of IoT to assess their knowledge and awareness among users of IoT. The mode of study was through a questionnaire sent through Google forms to a selection of Indians living across the U.S. The place was chosen as some of the authors were in that country and also because its usage is more in the U.S. Many homes have extensive use of IoT, even if it's for simple operations like turning on/off electric bulbs. Privacy issues have also been a matter of concern as these devices are linked to the internet. The sample was chosen from judgment /convenience sampling. Only one member per family was asked to respond so that there is no overlap of the collected data. The respondents were asked about the privacy issues of using IOT devices and also if it bothered them to continue usage. The results depicted that not only were users aware of the privacy issues related to IoT, but they also expressed concerns over the same. Due to the convenience and ease of usage, it is highly unlikely that people will stop using these devices but definitely, the usage will be more guarded in the future.

Keywords: Internet of Things; IoT; Privacy; Analysis; Statistics; Devices

1. INTRODUCTION

The Internet of Things is the fashionable term that refers to the multitude of devices that can be connected to the web. Through their connectivity, these gadgets can collect data on a variety of levels. The term "Internet of Things" (IoT) was termed for the very first time in a presentation given by Kevin Ashton during his explanation about implementing radio-frequency identification (RFID) used in the Procter and Gamble Company for an optimum utilization of supply chain management [1]. "The Internet of Things integrates the interconnectedness of human culture --

our 'things' -- with the interconnectedness of our digital information system -- 'the internet.' That's the IoT," Ashton told ZDNet. Tech analyst company IDC expected that in total, there would be overwhelming news of approximately 41.6 billion connected IoT devices by the year 2025, or "things." It also suggests the revolution that can be expected in the fields of industrial and automotive industry of connected "things or entities". It is also evident that we also foresee huge application of smart homes and wearable devices in future. Due to the increasing number of connected devices, the Internet of Things is expected to infiltrate and become a part of various aspects of daily life.

Unquestionably, IoT will have a significant impact on the lives of all members of society shortly. In 2020 alone, more than 50 billion devices were estimated to be involving IoT applications [20]. While its presence will be most significant in domestic life, it will also have a far-reaching impact on the industry [16]. IoT is the enabling technology in site-specific farming practices which have led to increased output along with more efficient processes [21]. IoT is also at the core of developing technologies that enable the implementation of Smart City projects [25]. Even in the field of medicine, IoT applications are rapidly gaining ground. While neurology, cardiology and psychiatry were subfields witnessing the most use of IoT prototypes, India, China and the US are the most involved countries in medical IoT research [26]. A centralized collection of data and decentralized and automated decision making through IoT devices are also being seen as the future of defence and military establishments [27].

Due to the nature of the Internet of Things concept, security and privacy concerns are very prominent, and various research challenges will occur [2]. This is because of the broad scope of its impact on multiple fields. Inadequate updates, security protocols, and user unawareness are major challenges facing the Internet of Things (IoT). Such issues are faced by families whose day-to-day activities depend on these devices. Moreover, it is very important to understand whether families using these devices are aware of the privacy issues that come along with them.

The research idea focuses on family cohorts to better comprehend the usage of various IoT devices amongst the family members based on their information. The data has been collected on the educational qualification, age group, family size, and employment status of the respondents.

The study mainly revolves around three vital problem statements which need to be accounted for:

a. How did the pandemic affect the dependency on IoT devices?Are people/the public aware of the privacy issues imbibed in these devices?
b. Is the privacy information attained causing any alteration in their usage pattern?

Why is the privacy of IoT devices significant?

As IoT becomes a part and parcel of people's lives, the monotonous work gets less tiring and more convenient. However, when people start to enjoy those comforts, they tend to neglect the hazard of their personal or professional data can be at stake.

The number of IoT devices is humongous. These digitally connected devices are well interconnected across the globe in order tofacilitate communication between connected devices. For example, appliances such as automobiles, domestic appliances used on a regular basis, televisions and many other I/O devices are collecting and as well as simultaneously transmitting the data across the channel of internet in order to complete the task assigned. Users are generally unaware of the quantity and characteristic of the data that is collected and shared with others. In the process of collecting and transferring the information among these well-connected devices and data recipients, there is always a security concern that prevails in the background which has to be dealt with diligence.

A security breach starts with a privacy breach. In order to protect and safeguard consumer data, The World Economic Forum (W.E.F) along with the Massachusetts Institute of Technology (M.I.T) and a white paper called "Realizing the Internet of Things: A Framework forCollective Action", which was published in 2018. Their common goal is to improve awareness and let the consumer make the final decision.

Possible privacy violations

The usage of IoT is undoubtedly the cool and trendy technology that has not just made life easy but has also reduced the overall energy consumption which also means less electricity bills. As consumers of such devices, we must be aware of what are the possible violations and the impact of those on our daily lives. When multiple non-computer devices are connected, the personal data that is collected has a higher value which tends to be misused.

1. When data such as time and duration of equipment working are tracked, we can predict the chain of daily activities of the family with a certain confidence.
2. Few correlations can be made between two likely incidents such as, your alarm time and the time when the geyser is turned on.With information from sensors that surround us always, real-time data can monitor and also control us. They do offer valuable insights to help optimize time, energy, and money.
3. Data is collected from commercial security systems and is used for monitoring unknown restricted entries or to check for any undesirable deeds of staff/customers and the management team.
4. Traffic tracking systems are used for tracking the culprit violating traffic rules, to find some root cause of the road accidents, in other police cases.
5. With IoT safety at the workplace is ensured for several factory workers who deal with manufacturing, construction machines that are risky and require much human attention.

Rules and Laws governing the protection of privacy of IoT

PR ICO end 2016 states a fact that 6/10 of IoT devices do not properly reveal to their customers how their personal information is stored/communicated and utilized. This means

60% of our activities are monitored without our permission.

The communication channels are carefully monitored by trusted organisations and inescapable rules have come up for our rescue. One such policy is the GDPR policy enforced by the European General Data Protection Regulation Committee. GDPR also includes the R.F.I.D tags.

2. LITERATURE REVIEW

The following are the list of scholarly articles, research work, conference papers, some sample surveys and their results along with a few publications that give us an understanding of existing research done in the field of IoT based on the privacy of data.

The defining features of IoT, its architecture and its applications have been studied extensively by Madakam et al. [3]. Scholarly analysis of extensively studied research and with detailed discussions to come up with an aggregation of basic requirements or characteristics and aliases of the IoT. They recognized that IoT was bringing a sea of change in various sectors of life but some flaws existed at the governance and implementation levels.

Lin and Bergman [4] establish that privacy concerns are dominant in IoT environments and differ significantly in domestic and industrial applications and hence require a differentiated approach in dealing with them. They recognize that the security of the networks depended on the installation and configuration by staff. The staff here we partially or untrained to handle the systens and so there was a proposal to support the gateway architecture by automatic devices.

Ukil et al. [5] focus on developing a reliable sensitivity detection system that is robust after analyzing the privacy content required for a genuine statistical disclosure for the information-theoretical model. They find that privacy-preserving data mining (PPDM). This method minimizes sensitive data disclosure probability to reasonable levels and standards. In reality, this method requires some intense remodeling as basic awareness of user's privacy policies are yet to be addressed in detail. As an alternative, the paper proposes a valid scheme in IoT systems which enable sensor data owners to assess the privacy risk of sharing their sensor data like smart meter data to authorised third party applications in pre-defined and accepted quantifiable terms.

Zheng et al. [6] gets in touch with the users of smart homeowners and generates primary data for analyzing the reason for purchasing IoT devices, their perception of a smart home, potential actions that can be undertaken in case of privacy breach and so on through a semi structured interview. Also tried to understand the opinions of the users to create, manage or monitor, track or check and regulate IoT devices their personal data. The interview results revealed that users trust IoT device manufacturers to protect their privacy. But unfortunately, they do not have clear understanding of privacy risk of the agreement that they have signed with the manufacturer of device, nor the tricky algorithms that operate on the privacy data used to capture the minds of the customer.

Hui et al. [22] review existing literature on frameworks to mitigate the privacy threats in IoT devices. In order to combine several real time systematic and simulations they considered a large-scale mobile network traffic to quantify IoT privacy leakage. This process was based on evaluating 47651 IoT devices. Based on the results exhibited, IoT devices in work spaces and commercial complexes have a higher scale of privacy leakage than independent and discrete users and platforms. The defined algorithms perform different daily patterns and simulate the environment to comprehend the privacy leakage idea. This again pre dominantlydepends on their working conditions.

Luo et al. [23] Currently, a privacy leakage analysis called ALTA enables us to infer running apps in smart home IoT environments. They develop unique and multiple fingerprints to differentiate running apps to work on privacy-sensitive aspects to comprehend and encode context-rich information from apps.

Van Kleek et al. [24] proposed a reliable method which initiates to build a smart home IoT devicesby introducing a concept of enriching privacy-empowering network disaggregation which would give the IoT device the right to share or collect the data? Therefore, the device is held accountable for their own disclosures. This disaggregation actively monitors and analyses all the network traffic passing into and out of the network connected regions, helping to build a visual atlas to end users to understand the overview of the functionalities of this complicated system.

Arabo et al. [7] suggested an unique framework for privacy and security in smart homes while also presenting early simulation results. They predict an exponential increase in the number of malware applications and related attacks. They propose an alternative framework to be implemented at Smart Homes. Those which addresses the key issues such as the three main security threats which is user privacy concerns, identity theft and personal content tracking. The proposed idea of design is an outcome of scientific research. The implementations have also been simulated in various environments and deployed. The model is tested and verified on various portable real-time devices. Those which use the available device emulators in the .NET development environment.

In a week-long study of five users, Worthy et al. [8] analysed the nature of human and socio-technical concerns among the users, who also own IoT devices. The study identifies trust as a critical factor and discusses designing IoT devices to encourage user trust. The study finds that the technology itself receded in participants' awareness. This suggested users may only hold the initial momentum to be cautious of the data share but not very mindful of the same over a period of time.

McCreary et al. [9] identify privacy as a potential barrier to end user in adoption of any technology. The researchers undertaking qualitative research with authors ideas of building and intelligent home/building, do pay attention to the monotonous usage of IoT devices, aware of the

information sensitivity attached to them and also study the network frame of these inter-connecting devices.

In their study, Martin and Nissenbaum [10] try to explain the divergence in the actions of consumers and the views regarding privacy as recorded by previous surveys. The researchers surveyed 569 individuals and his research revealed that the intention of collecting data was more rpersonal to users' privacy opinions than to the sensitivity of the data itself.

Lee and Kobsa [11] aim to understand how contextual parameters influence IoT users' perception of IoT scenarios. They surveyed 200 individuals to categorize IoT information collection and analyzed them using a K-model clustering algorithm. Of the parameters to which users were receptive, location-based service was found to be the most significant.

In a survey of 1007 participants, Emami-Naeini et al. [12] measured the privacy expectation levels in 380 IoT device use cases and explained a few of special scenarios. Apthorpe et al. [13] surveyed 1,731 individuals. Their perceived acceptability of 3,840 information or data points were collected. Few among these were a range of IoT devices, types of information, number of data recipients, and conditions data which data is collected.

Huacarpuma et al. [25] introduced a Distributed Data Service (DDS). The aim was to enable various IoT middleware systems and sub-systems to have a common data sharing platform. In order to collect and process data for IoT environments.

Abu-Elkheir et al. [26] surveyeda reliable solution using the data management framework. The proposed solutions are based on the working models for IoT or subsystems of the IoT devices. These working modulesare primitive in nature and highlight the distinctive design. The purpose of an exclusive IoT data management solution is thus obtained as detailed discussion on every element of the framework is done.

Alhazmi et al. [27] additional to the previously studied theory, that examines users' privacy expectations and their level of preferences for IoT devices. The main focus of this study is on examining users' feelings, reactions and responses regarding their data collection in an interconnected environment.The findings in this study support users' perceived benefit is an essential and key factor. In contrast to the previous study, the authors identified that the place of work, commercial entities havebeen a sensitive location for users are uncomfortable sharing their private information.

Mohsin,K [30] Users are typically unaware or partially blind of quantity and quality of data that is collected in real-time scenarios. It is very unfortunate that there is not much light on implications, use cases and relevance of data shared. As a result of the elaborate process of collecting and communicating the data among these inter connected devices and data recipients there is an

evident concern about data security.

Plageras et al. [31] examine the new age and trendy technologies such as Big Data, Cloud Computing, Machine learning tools and monitoring systems of IoT framework. The study suggestsvarious methods to combine their intelligence and functional abilities in order to have beneficial scenarios of their use.

Norihiro et al. [32] introduces basic concepts, key concepts related to Internet of Things (IoT) data privacy, and discusses the approaches to IoT data privacy. They describe the Privacy Preference Manager (PPM), which is awell inter-connected IoT data platform. This component is well accepted and sufficient to provide data privacy by registering users' consent and their privacy preferences. This is done by providing a defined and structured process to modify the existing rules for preferential data flow.

R Chow [33] is of the opinion that to ensure privacy is to give users a simplified way to discover and be constantly aware about the privacy properties and possible privacy based breaches of IoT services.

Gupta and Ghanavati [34] proposed a privacy protection framework for the IoT called HIPA (Heterogeneous IoT Privacy Architecture). This scientifically based architecture aims to resolve some of the privacy concerns that arise in a heterogeneous environment.

Lee and Ahmed [35] discussed the development of a new IoT model that can enhance the security and privacy of the users of IoT enabled devices. Their results indicate that the new model can be effective in addressing the expected needs of the IoT users.
Rathan Kumar [36] recognizes that there is an inherent trade-off between the privacy of users' data and the convenience offered by IoT devices. The paper cautions against misuse of such data warn of a "security catastrophe" if the privacy concerns are not addressed.

Xi and Ling [37] studies the key determinants of privacy security risks, and suggest some real time and new age relevant IoT risk prevention methods.

Shayegh et al. [38] analyze privacy policies of IoT devices. Their analysis reduces the length of a privacy policy and makes it organized based on privacy practices thus improving the level of understanding for the user.

The white paper on IoT published by the World Economic Forum [39] includes a framework that analyses the space, the opportunities for impact and the challenges facing the IoT ecosystem. Among the challenges highlighted by the paper are the concerns related to security and privacy of users' data.

Aleisa and Renaud [40] analyzed proposed solutions for preserving privacy with respect to the tools and techniques deployed.Also, the extent to which security principles of the core systemsof these procedures were satisfied.The findings showed that very few solutions satisfied the pre-defined, expected and basic privacy principles.

3. MATERIAL AND METHODS

The paper emphasizes and is based upon on a statistical analysis of empirical data collected through means of a sample survey. The data was collected using Google forms which were sent out to the public. The Google form had the following questions:

1. Please mention your name (Optional)
2. Please choose your age group
3. Kindly fill in your educational qualification
4. Your profession
5. Kindly indicate your family size
6. Which of these IoT devices do you have in your home? (Check all that apply)
7. Has lockdown increased your usage and dependency on IoT devices? (For, e.g. instead of getting up to switch on a light, do you ask your smart device to do it?)
8. Are you aware of the privacy issues involved in the usage of these devices?
9. Do these privacy issues bother you?

The responses to the above questions are used to answer the research problem by subjecting them to usual percentage analysis and elementary descriptive statistics. The response to each question has been classified based on age, employment, family size and education to gain perspectives on how these factors influence users' interaction with IoT. The same has been represented through bar diagrams.

Data Visualisation and IoT

Few among the ample tools to model and visualize the data captured and collected from the Internet of things (IoT) are, Kibana Tool, PowerBI, ThinkSpeak and DGLux. Data visualization helps the stakeholders make better-informed decisions as they deal with real-time data. When multi-dimensional data needs to be analyzed, visualization tools are effective in delivering meaningful insights.

4. OUR STORY

4.1 DATA CLEANSING

The survey originally received answers from 58 respondents. From these, 3 responses were repeated twice. Responses [20 and 19], [36 and 37] and [57 and 58] had similar entries under all the categories of questions asked with a minimum difference in the periods mentioned in

thetimestamp column. This can be because of double entries that are possible due to technical errors. Therefore the responses in rows 20, 36 and 58 are eliminated from the analysis in order to eliminate data repetition. Therefore, in this survey, the total responses put under analysis is 55. (58-3)

4.2 DATA AND ITS FEATURES

The general data categories of respondents are as follows. These categories classify the respondents into different groups that help the analyst understand the background information about the respondent like the category of age, family size, type of IoT device used, education qualification andemployment.
During analysis multiple aspects of this data is combined and analysed for better understanding of the user's idea behind the usage of IoT devices.

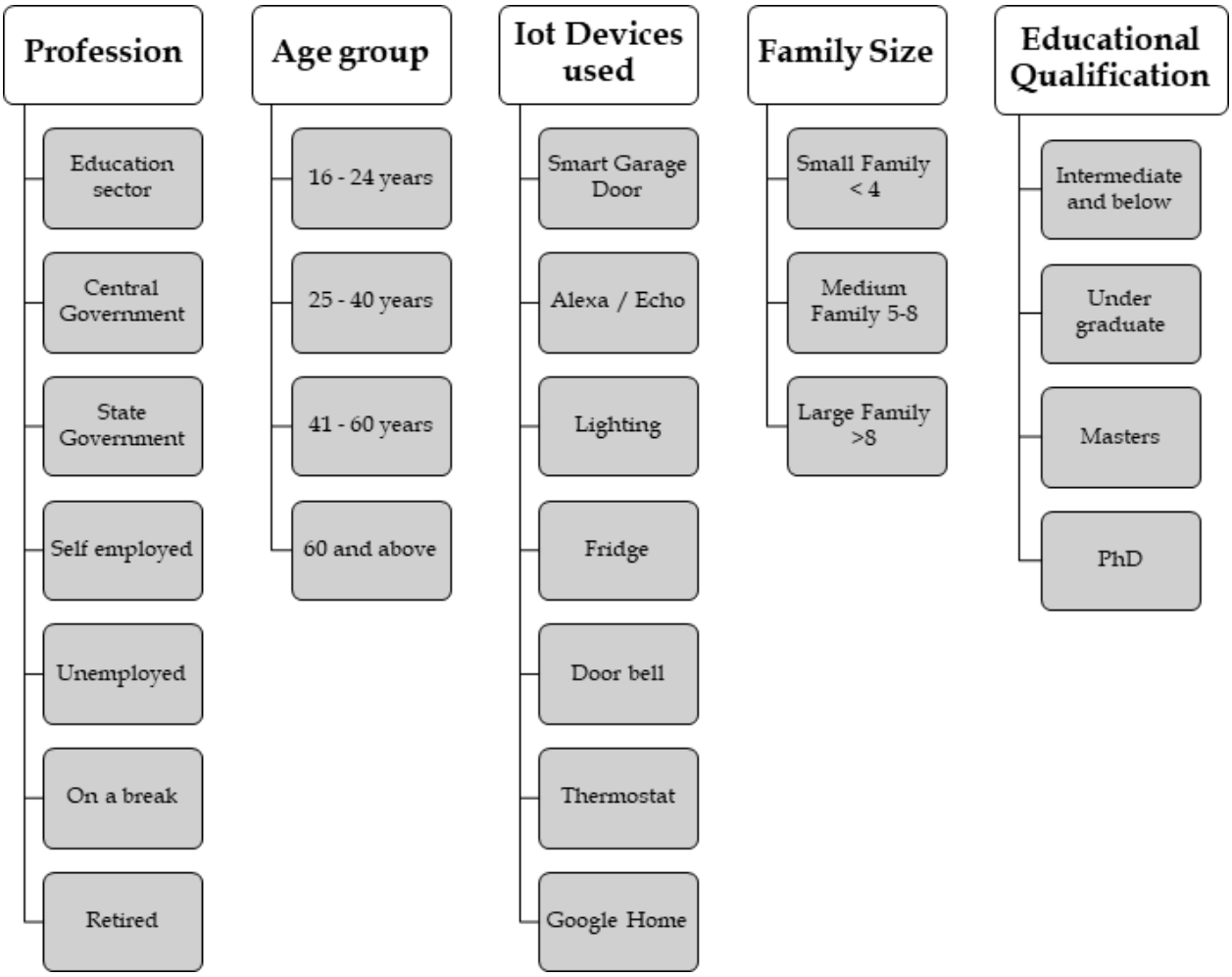


Fig1: Table that depicts the categories of information collected from the respondents.

Along with these general data points, we have collected information pertaining to the purpose of

the study where the respondents have to answer YES or NO format questions. Which are:

1. Has lockdown increased your usage and dependency on IOT devices? (E.g. instead of getting up to switch on a light, do you ask your smart device to do it?)
2. Are you aware of the privacy issues involved in the usage of these devices?
3. Do these privacy issues bother you?

The purpose of the survey is about privacy concerns among users of IoT devices. We have 4 options that the respondents might opt for, which are:

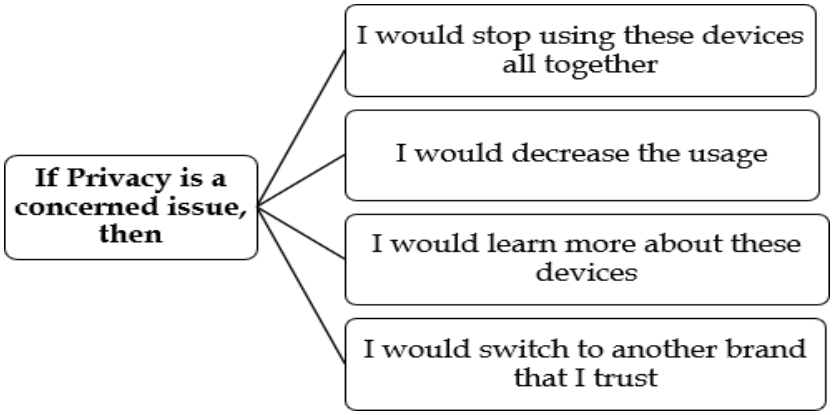


Fig 2: The possible options that user would chose if privacy was a concern.

4.3 STORY WITH DATA

So, let's first look at the variety of devices that the people from our survey are using. There are a total of 16 different types of devices that our respondents are accessing. Among the 55 respondents, 5 of them do not have any experience using an IoT device. This means that 50 respondents are using a total of 102 IoT devices in total.

As the treemap depicts, Alexa is unambiguously the most popularly used IoT device followed by the IoT devices that are used for lighting purposes at residential/commercial establishments and then by smart garage doors and so on. Alexa gets the credit among its customers because it's an intelligent voice assistant getting smarter at work and making it a worthwhile addition to smart homes. Even the macroeconomic facts about the global sales of Alexa are in line with the popularity of the brand among the people in our survey. By the last quarter of 2017, the total number of units sold went up to **21.5 million.** Fig 3 is a visual representation of the popularity of the device type.

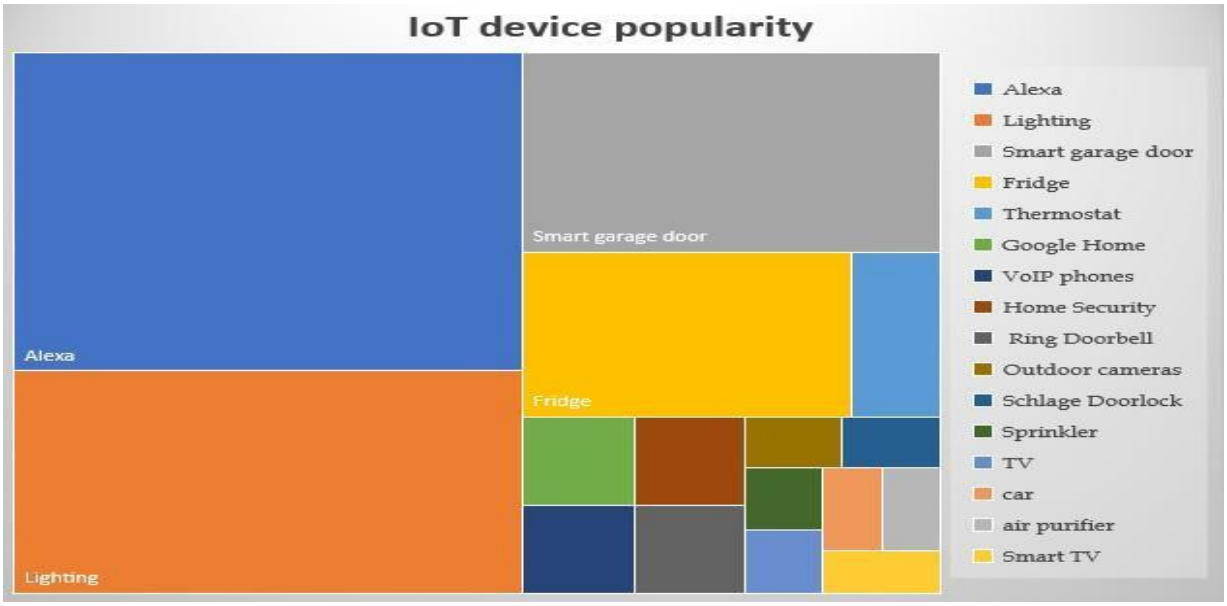


Fig 3: IoT device popularity

Now, let us look at the detailed statistics of the device's popularity and their usage.

Table 1 - IoT devices and their relative frequencies.

IoT devices and their relative usage			
Sl.No	**IoT Device**	**Users**	**Relative Frequencies**
1	Alexa	33	32%
2	Lighting	23	23%
3	Smart garage door	17	17%
4	Fridge	11	11%
5	Thermostat	3	3%
6	Google Home	2	2%
13	VoIP phones	2	2%
7	Home Security	2	2%
8	Ring Doorbell	2	2%
9	Outdoor cameras	1	1%
10	Schlage Doorlock	1	1%
11	Sprinkler	1	1%
12	TV	1	1%
14	Car	1	1%
15	Air Purifier	1	1%
16	Smart TV	1	1%
TOTAL		**102**	**100%**

From the relative frequency distribution table, we conclude that 32**%** (33 devices among 102 devices) of devices used by the respondents belong to Alexa, followed by IoT devices that enable easy operations on the lighting of the house/office of the respondents with a narrow difference of 23% and followed by the smart garage door, fridge and so on. Now, let us take note of the statistics related to the privacy concerns of the respondents using these devices. Consider the below bivariate table, tabulated with responses from the respondents about their awareness and concerns with respect to the privacy norms of the IoT devices that they are accessing. A total of 55 responses were considered.

Table 2 - Privacy concerns among the respondents.

		Do these privacy issues bother you?		
Are you aware of the privacy issues involved in the usage of these devices?		Yes	No	Total
	Yes	31	13	44
	No	5	6	11
	Total	36	19	55

This table provides a very meaningful picture of reality. The primary concern of this research is about these 31 (out of 55 around 56.36%) respondents who are aware of the privacy norms and are yet still not completely satisfied with their protection of privacy in using these IoT devices. This can be because of multiple reasons such as,

1. For any individual, it is a challenging task to understand and acknowledge all the nuances in the terms and conditions agreement of the IoT ecosystem.
2. Every update, there can be a possible compromise on data sharing.
3. Weak passwords which are liable to security breaches.
4. Insecure interfaces and poor IoT management.
5. Eavesdropping

Also, there are 23.63% (13/55) of them who feel they have been well informed about the privacy protocols and are happy customers of the IoT devices that assist them. 80% (44/55) of our respondents are cautious and mindful about the privacy protocols of the digitally smart devices they are associated with. Whereas, the remaining 20% of them are in the dark. It's definitely time for action, we need to accumulate several concerted efforts in educating the customers about the vulnerabilities and possible threats that can be expected with their privacy being compromised.
"Through 2018, over 50% of IoT device manufacturers will not be able to address threats from weak authentication practices" – Gartner .

Even Intel Security surveyed to identify the risky behaviours of consumers who areeager to buy digital products during the holiday season. We must understand the importance of educating this crowd to rethink on their decision. A popular macroeconomic study reveals that,

Fig 4: Security measures among the users of digital devices.

Source: https://www.businesswire.com/news/home/20161120005023/en/McAfee-Survey-Reveals-42-Percent-Consumers-Proper

Let us consider the case of the 11 respondents who are not exercised their right to product information. To our surprise, 6 out of 11 (54.54%) respondents have been credited with a master's degree. Very few middle-sized and large-sized families are vulnerable due to ignorance, but yet again 8 out of 11 families (72.72%) are of them belong to small families with less than 4 members in the house. We must take note that more than 50% (54.54%) of the total clueless respondents belong to a small family with a master's degree in hand.

Table 3 - Family size and qualification of respondents who are ignorant of the privacy issues.

Family size/ Education Qualification	Intermediate and below	UG	Masters	PhD	TOTAL
Small family(<4)	0	1	6	1	8
Middle sized family (5-8)	1	0	1	0	2
Large family (>8)	0	0	1	0	1
TOTAL	1	1	8	1	11

Let us study the possible path that the respondents opt for when they are concerned about their privacy. (Who have said YES to the question “Do the privacy issues bother you?” in the survey) There are a total of 36 replies of YES. Removing the two blank entries, we have 34 opinions that are categorized as follows:

Table 4 - Privacy protection measures by the respondents.

I am concerned about my privacy in usig Iot devices. So,	Count
I would learn more about these devices	16
I would switch to another brand which I trust	4
I would stop using these devices altogether	3
Would like to see Increased security for these devices	2
Grand Total	**34**

As per the consumer protection laws, the right to product information is our fundamental duty. 47.05% (16/34 respondents) have recognized their rights and are keen on better security information. The number under consideration in Table 4 is that 72.72% of them (32/44) have a decent education qualification to understand that they can help combat these attacks by ensuring their devices are updated in a timely manner. This way, it aids in mitigating risks from the latest and certain specific threats that can be unknown at times.

Table 5 - Family size and education qualification of respondents who are aware of the privacy issues

Family size/ Education Qualification	Intermediate and below	UG	Masters	PhD	TOTAL
Small family(<4)	0	7	30	3	**40**
Middle sized family (5-8)	0	2	1	0	**3**
Large family (>8)	0	0	1	0	**1**
TOTAL	**0**	**9**	**32**	**3**	**44**

Impact of lockdown

It is very evident that covid-19 has brought good news to a few technology companies with an unexpected and overwhelming increase in their adoption. This is due to the fact that people are forced upon becoming digitally smart to cope up with the current situation. Let us understand if this lockdown 2019 is having an unprecedented impact on our respondents.

In the questionnaire, the responses to the question, "Has lockdown increased your usage and dependency on IOT devices?" have been analyzed with respect to the profession and their age. Certain professions demanded people to get more acquainted with digital devices. In general, the age factor and dependency levels are expected to be proportional to each other. Therefore, Table 6 is a multivariate table (3 variables) depicting a total of 55 responses categorized across age, profession and the opinion of respondents on lockdown increasing the dependency on IoT devices. We notice that 25 and 30 respondents agreed and disagreed on their increase in dependencies respectively. This means more or less the opinions were equally divided among the respondents.Also, majority of the respondents, (36 out of 55 respondents, 65.45%) occupation is in the private sector.Unemployment or a break in career has absolutely no impact on the increase/decrease of usage of IOT devices during the lockdown.

Table 6 - Understanding the impact of lockdown based on age and profession of the respondents.

Impact	Profession	16-24 years	25-40 years	41 - 60 years	60 and above	TOTAL
YES	Student	0	0	0	0	**0**
	Private	0	14	3	0	**17**
	Self employed	0	2	0	0	**2**
	Central government	0	0	0	0	**0**
	Education sector	0	0	2	0	**2**
	Unemployed	0	0	0	0	**0**
	On a break	0	0	0	0	**0**
	Others	0	3	1	0	**4**
TOTAL		**0**	**19**	**6**	**0**	**25**
NO	Student	1	0	0	0	**1**
	Private	0	13	5	1	**19**
	Self employed	0	1	0	0	**1**
	Central government	0	0	1	0	**1**
	Education sector	0	0	3	0	**3**
	Unemployed	0	1	0	0	**1**
	On a break	0	0	1	0	**1**
	Others	0	1	2	0	**3**
TOTAL		**1**	**16**	**12**	**1**	**30**
GRAND TOTAL		**1**	**35**	**18**	**1**	**55**

As per the responses received, when ‘age’ as a factor is considered for analysis. We notice that just 2 out of 55 responses have been made in the early age category of 16-24 and the older age category of 60+ years. This means, we are predominantly analyzing the impact of lockdown on the middle age categories of 25-40 and 41 to 60 years.

Based on the data presented in table 6, the impact of increased usage of IoT devices during lockdown seems to almost equally spread among the opinions YES (25) and NO (28).

How are your customers satisfied?

Considering the top 3 different IoT products that are popular among our users, we have listed the number of users who fell who have issues with their privacy. To our surprise, in this graph, it clearly shows that more than 60% of users in all the 3 scenarios have been worried about their privacy. This means there is a lot of scope for this research project to take in charge of immediate actions, protocols and set guidelines to tackle privacy issues.

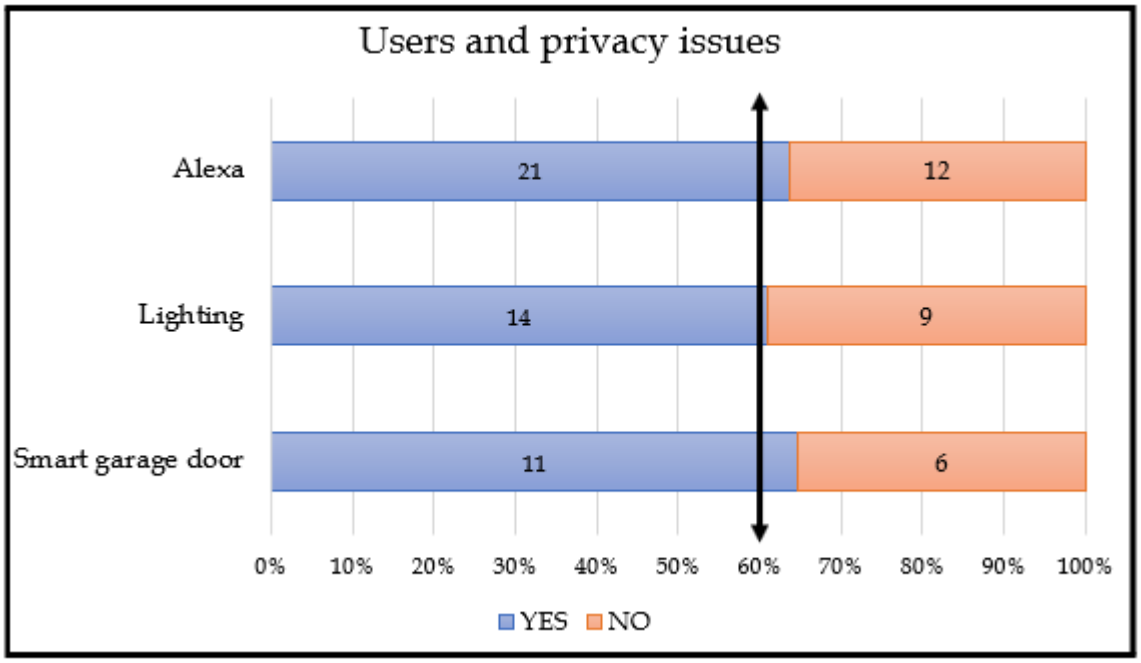


Fig 5: Devices used by different users and their current opinion on privacy concerns

5. DISCUSSION

5.1. Impact of Pandemic on IoT Usage

Other general graphs and their interpretations for the questions from the survey

1. **Has lockdown increased your usage and dependency on IoT devices?**

Age group

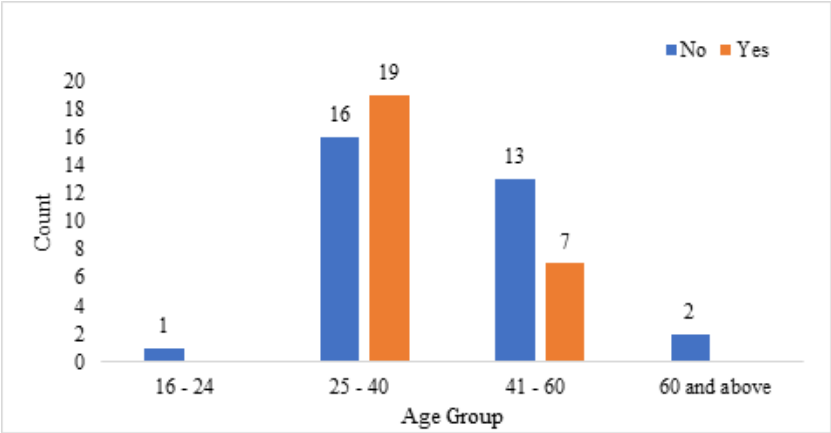


Fig 6: Age group Vs. Responses

From our survey, according to Fig 6, we observe that respondents in the age group 25-40 felt an increase in the usage of IoT devices during the pandemic, while the respondents from the other age groups do not share the same notion. The younger generation filled with enthusiasm and curiosity made good use of pandemics to explore and experience the IoT devices with time in hand.

Educational Qualification

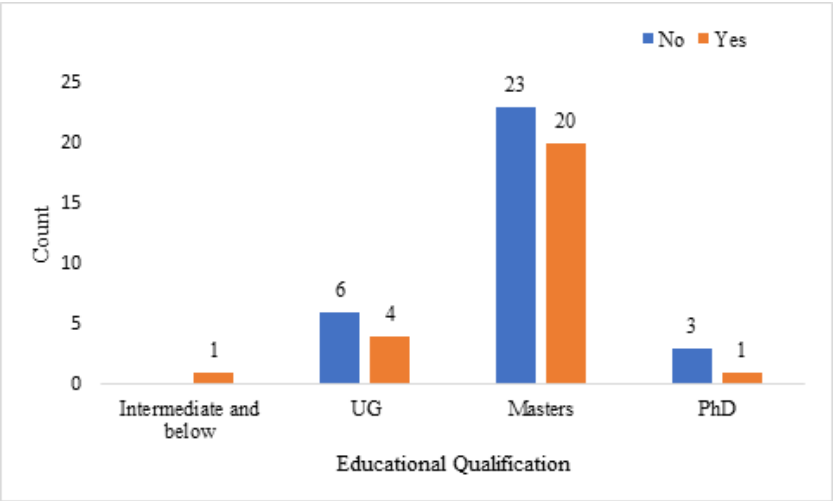
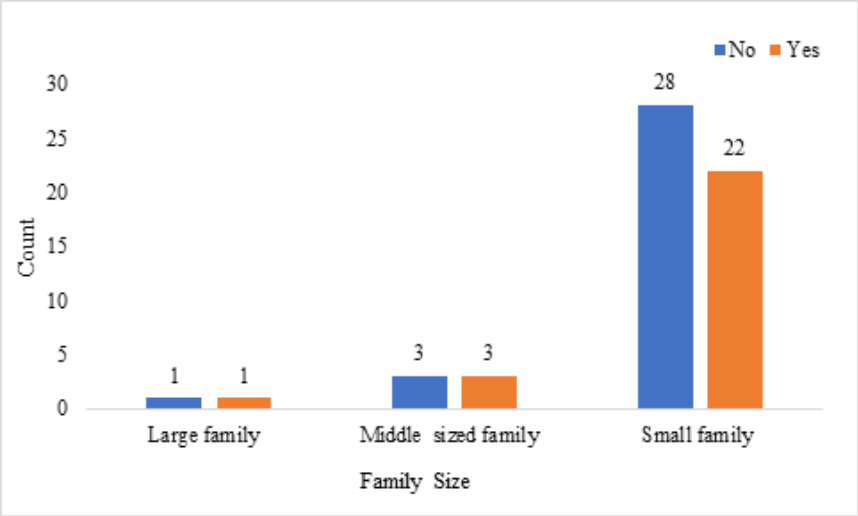


Fig 7: Educational Qualification vs. Responses

From Fig 7, we observe that the students falling in various educational categories felt not much usage or dependencies on the IoT devices during the lockdown. In this sample study, the variable "educational category" did not have a significant impact on the dependencies of IoT devices. The lockdown kept students busy with the transition from offline to online classes.

Family size



\

Fig 8: Family Size vs. Responses

Also, from Fig 8, we observe that most respondents with a small family felt there was not much usage of IoT devices in the pandemic compared to middle and large-sized families. This is because usage depends on requirements and family size. These two variables (family size and requirement) are proportional to each other. Higher the family size, the more the requirements of intelligent devices.

Profession

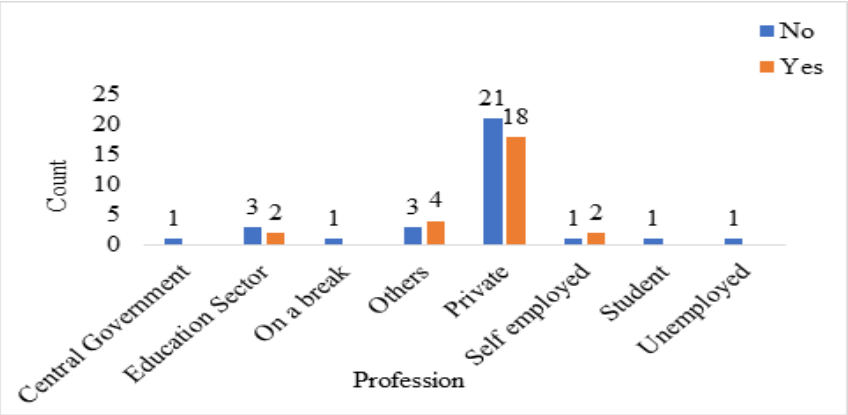


Fig 9: Profession vs. Responses

From Fig 9, we observe that most of the respondents who are private employees did not feel an urge to increase the usage and dependencies on these devices. As we already observed from Fig 3, the small-sized families feel that there was not much increase in the usage of IoT devices during the lockdown. This could be due to their awareness of the privacy issues involved in using these devices.

5.2 Privacy Concerns Regarding IoT

2. Are you aware of the privacy issues involved in the usage of these devices?

Age Group

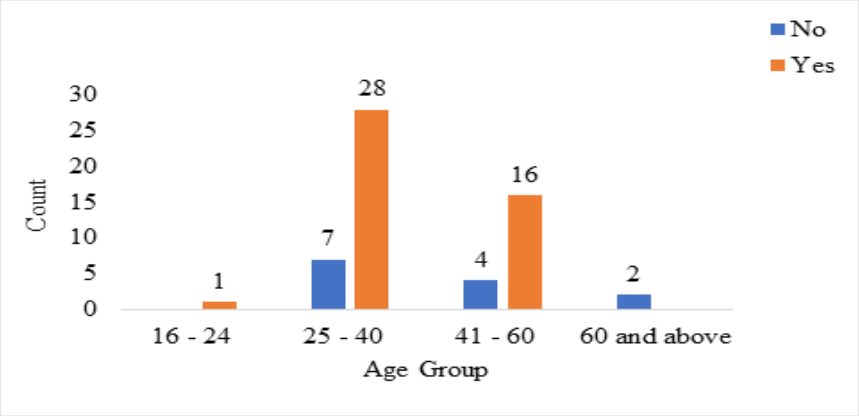


Fig 10: Age group Vs. Responses

From Fig 10, we observe that almost all the age groups except senior citizens (i.e., 60 and above) admitted that they are well aware of the privacy issues involved in using these devices. The majority of these people lie in the age group 25-40, followed by 41-60. This is proof that the younger and more educated group of the population is always given the right or responsibility of handling new technology.

Educational Qualification

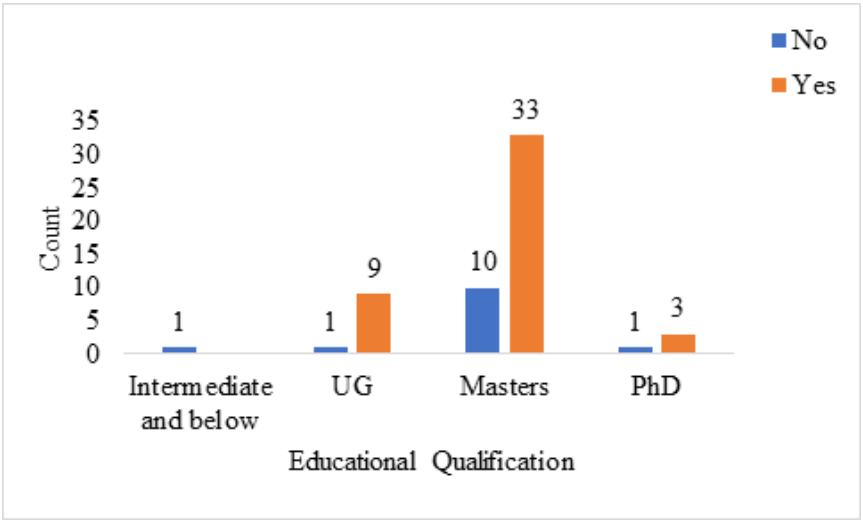


Fig 11: Educational Qualification vs. Responses

From Fig 11, we observe that most people with a degree admitted to knowing the privacy issues involved in the usage of IoT devices. This is evidence of how education brings awareness among people.

Family Size

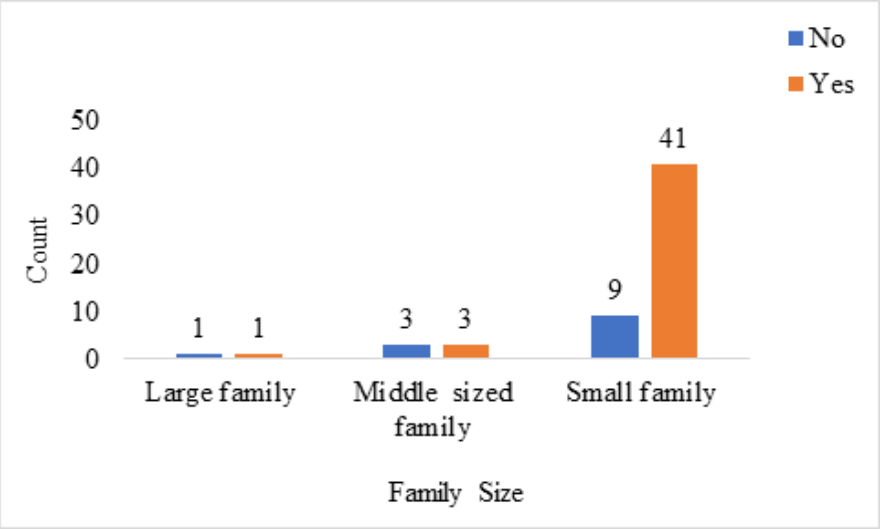


Fig 12: Family Size vs. Responses

As we already observed that the small-sized families feel that there was not much increase in the usage of IoT devices during the lockdown. This could be due to their awareness of the privacy issues involved in using these devices, as shown in Fig 12.

Profession

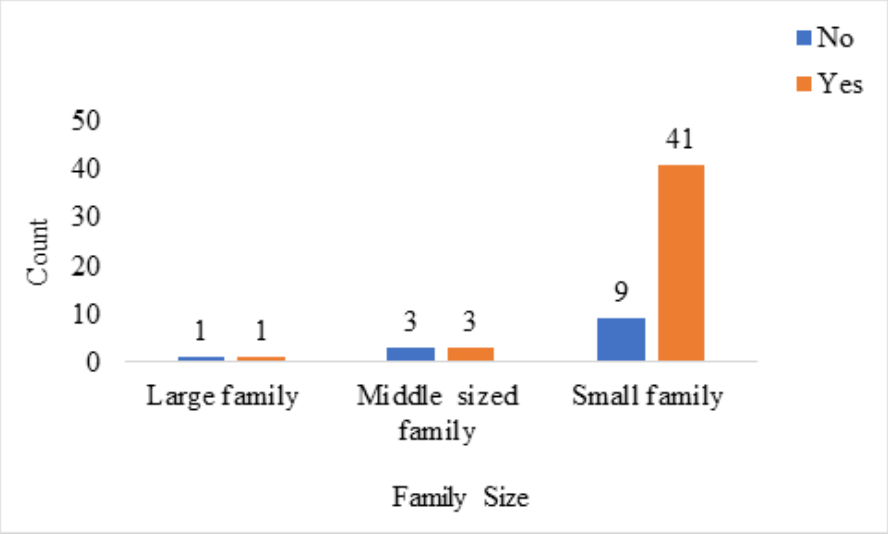


Fig 13: Profession vs. Responses

From Fig 13, we can see that the majority of the respondents aware of the privacy issues are coming from the private sector, which could be because of the environment they are working in. The private sector's environment encourages the employees to have a safe and holistic approach towards any decision making, which helps them wisely choose the devices they use.

3. Do these privacy issues bother you?

Age Group

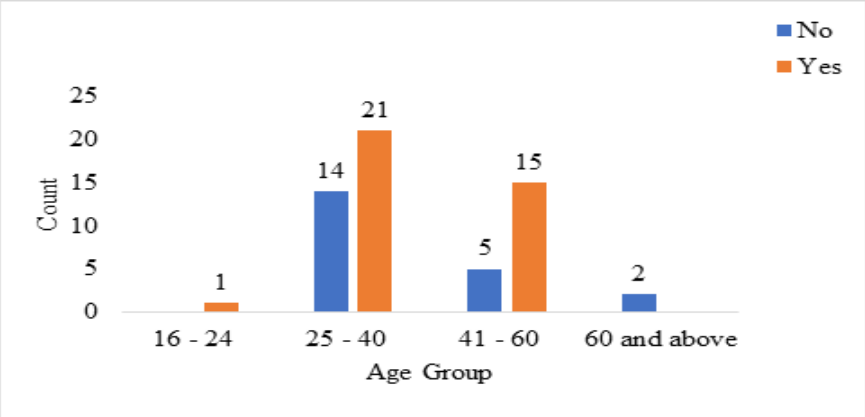


Fig 14: Age group Vs. Responses

From Fig 14, we can notice that majority of respondents belong to the age group of 25-40. Followed by people from age group of 41-60. Out of a total of 55 respondents, 37 of them are concerned about privacy.

Educational Qualification

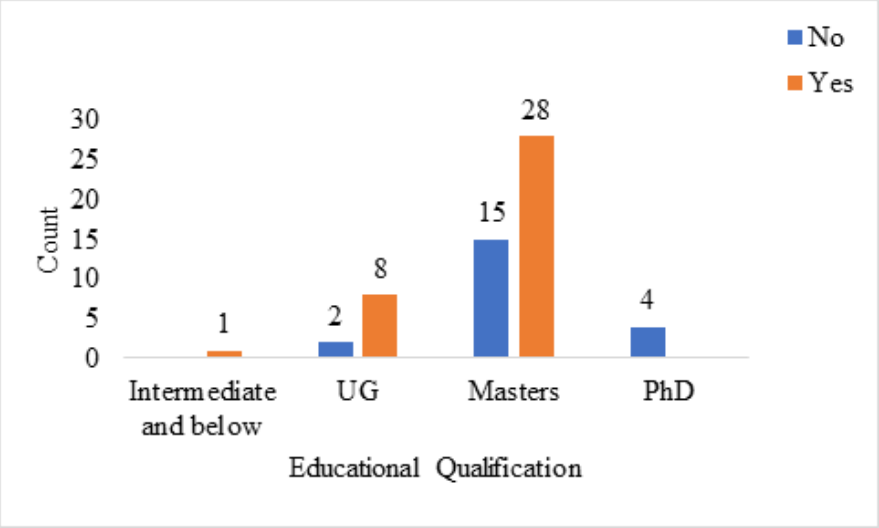


Fig 15: Educational Qualification vs. Responses

From Fig 15, we can notice that majority of respondents from our survey are well educated with a minimum of Undergraduate degree. Which means they are qualified to understand the terms and conditions mentioned in IoT devices and are capable of making a decision based on the privacy hazards of the device that they are connected to.

Family Size

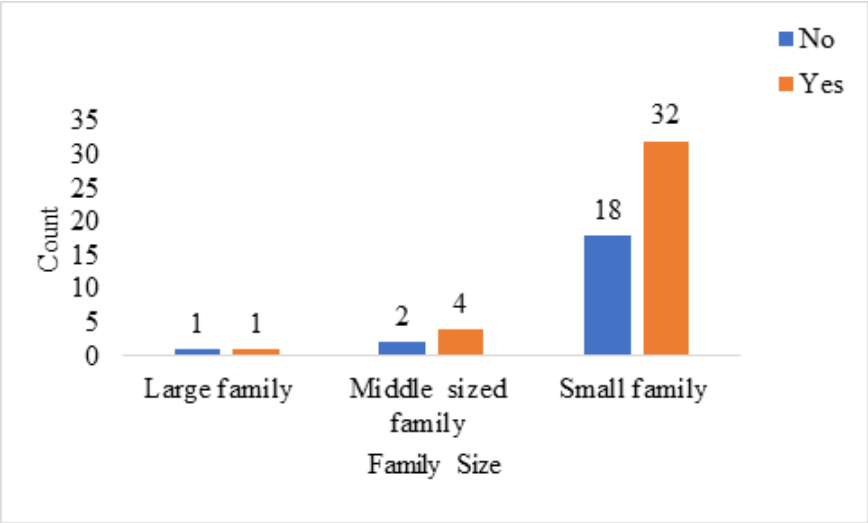


Fig 16: Family Size vs. Responses

From Fig 16, we notice that majority of respondents belong to a small family and so we can also estimate that the dependency on the devices are lesser when compared to that of a large family. A total of 90% (50/55) of the respondents belong to small family.

Profession

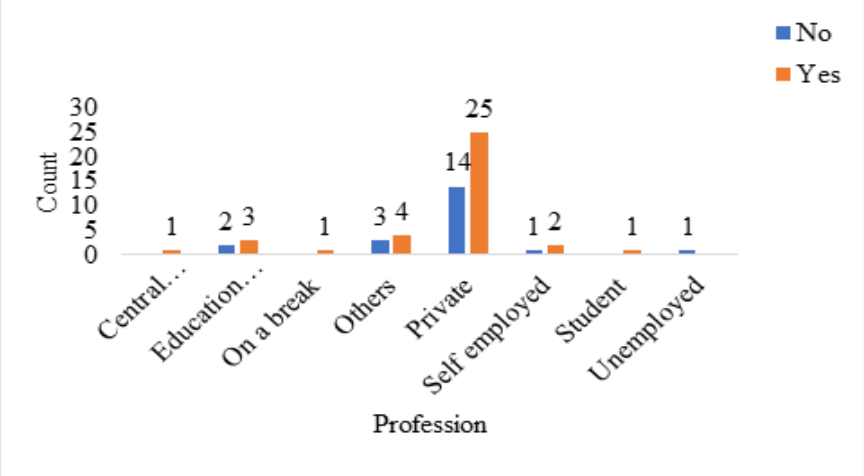


Fig 17: Profession vs. Responses

From Fig 17, we can notice that majority of respondents are from Private Sector. Also 64% (25/39) of them are concerned with the privacy of IoT devices that they are using.

5.3 IoT Usage Patterns

From Fig 18, while Alexa/Echo form the single largest use of IoT, its primary usage can be found in utilities like lighting, fridge, doors, among others, which, when combined, contribute the largest share. Also, Alexa's sales are positively correlated with their marketing and promotional tools. There were 53.6 million Amazon Echo shipments worldwide in 2020.

Which of these IoT devices do you have in your home?

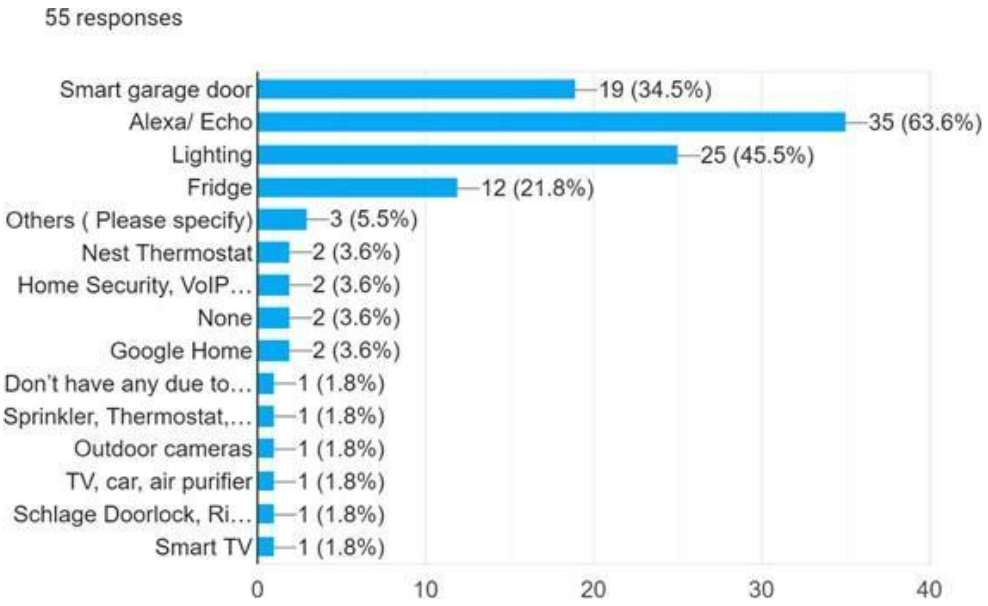


Fig 18: Types of IoT devices used by the respondents

5.4 Prospective Analysis

In addition to the analysis done, further studies can address both the positive and negative effects of privacy of IoT devices in other phenomena. Also, higher-order analytical tools can be used to make sense of complicated data.

As and when the sample size increases the analysis gets more evidence and significant conclusions can be made. Many statistical tools such as dispersion, regression, correlation with simulations and concepts in operational research can be applied to gain valuable insights.

- Streaming analytics uses an "in motion" dataset to analyses continuous data like live streaming and processing.
- Spatial analytics is the most important tool that analyses the relationship between two

physical entities and how they change over geographically defined areas.

- Time series analysis can be used to handle location and status data.
- With these, prescriptive analytics is mandatory to decipher large amounts of information/ evidence and deduce them to a meaningful and statistically significant conclusion.

The invention, progress and the development in usage patterns of IoT have created multiple benefits for many businesses and individuals in various aspects. However, as the IoT continues to evolve and it is the trendy tech that everyone wishes town it, certain expected threats and vulnerabilities are a part and parcel of this use case.

6. CONCLUSION

The paper establishes that IoT as a technology is used extensively by the public, with its usage having gained a significant increase post the incidence of the pandemic. It has also been shown that privacy concerns are prominent among the users of IoT enabled devices. While the extent of this concern varies with different demographic factors, their existence cannot be ignored. “Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built, enabling us to create boundaries and protect ourselves from unwarranted interference in our lives.”

Based on the sample collected, we can notice that most of them are aware of the disclaimer before operating the IoT devices. Even after agreeing upon the elaborate terms and conditions and also with the constant change of time, people are not well trained or warned against the probable misuse of their personal data against them. The findings of this study highlight the need for developing frameworks that address these concerns at levels including technology, policy, etc. in an assuring manner.

7. REFERENCES

1. Ashton, K. (2009). That ‘internet of things’ thing. RFID Journal, 22(7), 97-114.
2. Weber, R. H. (2015). Internet of things: Privacy issues revisited. Computer Law & Security Review, 31(5), 618-627.
3. Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.
4. Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. Information, 7(3), 44.
5. Ukil, A., Bandyopadhyay, S., & Pal, A. (2014, April). IoT-privacy: To be private or not to be private. In 2014 IEEE Conference on Computer Communications Workshops

(INFOCOM WKSHPS) (pp. 123-124). IEEE.
6. Zheng, S., Apthorpe, N., Chetty, M., &Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-20.
7. A. Arabo, I. Brown and F. El-Moussa, "Privacy in the Age of Mobility and Smart Devices in Smart Homes," 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing, 2012, pp. 819-826, doi: 10.1109/SocialCom-PASSAT.2012.108.
8. Worthy, P., Matthews, B., &Viller, S. (2016, June). Trust me: doubts and concerns living with the Internet of Things. In Proceedings of the 2016 ACM conference on designing interactive systems (pp. 427-434).
9. McCreary, F., Zafiroglu, A., & Patterson, H. (2016, July). The contextual complexity of privacy in smart homes and smart buildings. In International Conference on HCI in Business, Government, and Organizations (pp. 67-78). Springer, Cham.
10. Martin, K., &Nissenbaum, H. (2016). Measuring privacy: an empirical test using context to expose confounding variables. Colum. Sci. & Tech. L. Rev., 18, 176.
11. Lee, H., &Kobsa, A. (2016, December). Understanding user privacy in Internet of Things environments. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 407-412). IEEE.
12. Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., &Sadeh, N. (2017).Privacy expectations and preferences in an IoT world. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 399-412).
13. Apthorpe, N., Reisman, D., &Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. arXiv preprint arXiv: 1705.06805.
14. Mayer, C. P. (2009). Security and privacy challenges in the internet of things. Electronic Communications of the EASST, 17.
15. Ziegeldorf, J. H., Morchon, O. G., &Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742.
16. Bandyopadhyay, D., &Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless personal communications, 58(1), 49-69.
17. Asghari, P., Rahmani, A. M., &Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. Computer Networks, 148, 241-261
18. Choe, E. K., Consolvo, S., Jung, J., Harrison, B., &Kientz, J. A. (2011, September). Living in a glass house: a survey of private moments in the home. In Proceedings of the 13th international conference on Ubiquitous computing (pp. 41-44).
19. Cranor, L. F., &Sadeh, N. (2017). Privacy expectations and preferences in an IoT world. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 399-412).
20. Zeinab, K. A. M., &Elmustafa, S. A. A. (2017). Internet of things applications, challenges and related future technologies. World Scientific News, 2(67), 126-148.
21. Zhang, L., Dabipi, I. K., & Brown Jr, W. L. (2018). Internet of Things applications for

agriculture. Internet of things A to Z: technologies and applications, 507-528.
22. Hui, S., Wang, Z., Hou, X., Wang, X., Wang, H., Li, Y., & Jin, D. (2021). Systematically quantifying IoT privacy leakage in mobile networks. IEEE Internet of Things Journal, 8(9), 7115-7125. doi:http://dx.doi.org/10.1109/JIOT.2020.3038639
23. Luo, Y., Long, C., Hu, H., Peng, G., & Yao, D. (2021). Context-rich privacy leakage analysis through inferring apps in smart home IoT. IEEE Internet of Things Journal, 8(4), 2736-2750. doi:http://dx.doi.org/10.1109/JIOT.2020.3019812
24. Van Kleek, M., Seymour, W., Binns, R., Zhao, J., Karandikar, D., &Shadbolt, N. (2019). IoT refinement: Making smart home devices accountable for their data harvesting practices. Stevenage: The Institution of Engineering & Technology. doi:http://dx.doi.org/10.1049/cp.2019.0134
25. Cruz Huacarpuma R, De Sousa Junior RT, De Holanda MT, De Oliveira Albuquerque R, GarcíaVillalba LJ, Kim T-H. Distributed Data Service for Data Management in Internet of Things Middleware. Sensors. 2017; 17(5):977. https://doi.org/10.3390/s17050977
26. Abu-Elkheir, M., Hayajneh, M. and Ali, N., 2013. Data Management for the Internet of Things: Design Primitives and Solution. Sensors, 13(11), pp.15582-15612.
27. Alhazmi, A., Kilani, G., Allen, W. and OConnor, T., 2021. A Replication Study for IoT Privacy Preferences. 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS),.
28. Monares, Á., Ochoa, S., Santos, R., Orozco, J. and Meseguer, R., 2014. Modeling IoT-Based Solutions Using Human-Centric Wireless Sensor Networks. Sensors, 14(9), pp.15687-15713.
29. Kumar, S., Tiwari, P. and Zymbler, M., 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1).
30. K. Mohsin, “IoT & privacy – issues in modern world,” SSRN Electron. J., 2021.
31. Plageras, A., Psannis, K., Stergiou, C., Wang, H. and Gupta, B., 2018. Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. Future Generation Computer Systems, 82, pp.349-357.
32. NorihiroOkui; Vanessa Bracamonte; ShinsakuKiyomoto; Alistair Duke, "IoT Data Privacy," in The Internet of Things: From Data to Insight , Wiley, 2020, pp.121-139, doi: 10.1002/9781119545293.ch10.
33. R. Chow, "The Last Mile for IoT Privacy," in IEEE Security & Privacy, vol. 15, no. 6, pp. 73-76, November/December 2017, doi: 10.1109/MSP.2017.4251118.
34. Gupta, S. and Ghanavati, S., 2020. Towards a heterogeneous IoT privacy architecture. Proceedings of the 35th Annual ACM Symposium on Applied Computing,.
35. Lee, C. and Ahmed, G., 2021. Improving IoT Privacy, Data Protection and Security Concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1), pp.18-33.

36. Rathan Kumar, R., 2017. Internet of Things ('IOT') - Privacy Concerns. SSRN Electronic Journal.
37. Xi, W. and Ling, L., 2016. Research on IoT Privacy Security Risks. 2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII),.
38. Shayegh, Parvaneh& Jain, Vijayanta & Rabinia, Amin &Ghanavati, Sepideh. ,2019- Automated Approach to Improve IoT Privacy Policies.
39. World Economic Forum. 2022. Realizing the Internet of Things: A Framework for Collective Action. [online] Available at: <https://www.weforum.org/whitepapers/realizing-the-internet-of-things-a-framework-for-collective-action> [Accessed 5 April 2022].
40. Aleisa, N. and Renaud, K., 2017. Privacy of the Internet of Things: A Systematic Literature Review. Proceedings of the 50th Hawaii International Conference on System Sciences (2017),.