Hindawi
Mobile Information Systems
Volume 2022, Article ID 4247651, 11 pages
https://doi.org/10.1155/2022/4247651

Research Article

Promoting Information Privacy Protection Awareness for Internet of Things (IoT)

Prominent Mugariri,[1] Hanifa Abdullah,[1] Miguel García-Torres,[1] B. D. Parameshchari,[2] and Khalid Nazim Abdul Sattar[3]

[1]*School of Computing, College of Science, Engineering and Technology (CSET), University of South Africa (UNISA), Florida, Roodepoort, Johannesburg, South Africa*
[2]*Department of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka 560064, India*
[3]*Department of CSI, College of Science, Majmaah University, Al Majmaah 11952, Saudi Arabia*

Correspondence should be addressed to Miguel García-Torres; mgarciat@upo.es

Received 9 July 2022; Revised 6 August 2022; Accepted 17 August 2022; Published 16 September 2022

Academic Editor: Praveen Kumar Reddy Maddikunta

The Internet of Things (IoT) has had a considerable influence on our daily lives by enabling enhanced connection of devices, systems, and services that extends beyond machine-to-machine interactions and encompasses a wide range of protocols, domains, and applications. However, despite privacy concerns shown by IoT users, little has been done to reduce and protect individual information exposure. It is extremely difficult to mitigate IoT devices from reidentification threats which is why it is still a major challenge for IoT users to securely protect their information. The trust controls how we regulate privacy in our IoT platforms in the same way that it governs personal relationships. As IoT devices become increasingly linked, more data is shared across individuals, businesses, governments, and ecosystems. Technologies, sensors, machines, data, and cloud connections all rely largely on trust relationships that have been formed. With the rapid growth of additional types of IoT devices that are being introduced, it, therefore, expands privacy concerns and is difficult to develop trust with an IoT system or device without the option to regulate information privacy settings. Privacy has always been a barrier for many devices as they race for the early adoption of IoT technologies. Several Internet of Things devices or systems will continue to pose privacy threats. As a result, the main objective of this study was to examine the individual understanding of privacy and to promote information privacy protection awareness not only to IoT users but also to organizations that use IoT devices or platforms to run their day-to-day business operations. Furthermore, the objective extends to compare user knowledge and concerns about IoT privacy, as well as to identify any common attitudes and variances. However, in terms of enhancing individuals' knowledge, an artifact was developed to educate and enhance information privacy awareness among IoT users. A pre- and postquestionnaire was generated to test and validate user knowledge regarding information privacy protection in IoT. The study was conducted using a quantitative research method. Findings indicate that IoT users' awareness of information privacy protection turned out to be average, suggesting a need for education and awareness. Several participants stated that information privacy protection awareness is required within the community to educate, raise awareness, eliminate human error, and enable individuals to be conscious of their privacy when surfing the Internet.

1. Introduction

The Internet of Things (IoT) envisions the networking of billions to trillions of smart items around us that are uniquely identified and addressable everyday things capable of collecting, storing, processing, and communicating information about themselves and their physical surroundings. IoT systems will provide sophisticated services of a whole new sort based on progressively fine-grained data collecting in a densely populated ecosystem of smart objects. Pervasive healthcare, enhanced building management systems, smart city services, public surveillance, data collection,

and participatory sensing applications are examples of IoT systems. IoT is evolving as an Internet-based industrial information architecture used to simplify information flows among several platforms including supply chain networks. IoT is important in supply chain management because it streamlines supply chain operations, provides real-time information, and tracks business activities at multiple levels. Many new prospects for integrating IoT to several platforms exist today or might be anticipated soon. In order to fulfill these demands, IoT and its relevant supporting platforms must be swiftly established and designed in such a way that will promote information privacy protection.

The collecting, processing, and distribution of data amid people's private lives are becoming increasingly invisible, dense, and ubiquitous, raising severe privacy issues. Ignorance of these concerns might have unintended repercussions, such as nonacceptance and failure of new services, reputational harm, or costly litigation cases. Even if people are privacy conscious, the so-called privacy paradox demonstrates that they do not act in accordance with their stated beliefs [1]. One of the key challenges in such an interconnected digital world of modern technology is individual awareness, information privacy protection, and the ethical use of IoT platforms and applications. IoT helps enterprises reconsider their approach to their businesses to improve company policies. This has led to the majority of enterprises migrating from legacy or traditional systems to more integrated IoT systems that enable them to stay competitive and deliver better services to their customers. IoT is extensively utilized in manufacturing, transportation, and utility businesses, whereby detectors and many other smart devices are used [2]. Nevertheless, it has also found examples of applications for agricultural, infrastructure, and smart homes, leading to digital transformation for some organizations. Even though numerous concepts have previously been prototyped in field trials, it is difficult to forecast the repercussions of such widespread computer integration in this digital era. Lamba [3], as massive amounts of data, are exchanged and processed every hour or day; there is an extremely high possibility of IoT devices and services being vulnerable to some level of threats and cyberattacks. With these threats and attacks, it is important to investigate if individuals and organizations have enough information regarding their privacy protection. This brings us to the question, "Are individuals aware of their information exposure and protection on IoT planforms?."

While IoT is helping to make life easier for everyone, it is also necessary to think about how these attacks might be mitigated or avoided [4]. However, technology, such as smart homes, and e-health enable a wide range of processes throughout the integrated system's physical and virtual environment [5]. Professionals use their skills and knowledge to assist and defend users since individuals or users are increasingly vulnerable to security threats and attacks as daily activities progress. Verification, information management, setup, and authentication are all privacy concerns in IoT interconnected networks [6]. Although IoT products make life easier and more competitive, privacy is not guaranteed. Therefore, it is important to consider privacy and IoT as two variables integrated to work hand in hand to protect and create a level of trust when information is being exchanged. Even though they are not compatible, privacy helps separate confidential information while IoT connects all smart devices together. Privacy threats can be triggered in different ways between IoT systems. Endpoints in the IoT ecosystem broadcast data autonomously, but they also collaborate and interact with other endpoints. Internet of Things must be interoperable for networked devices to work seamlessly together. The data transmitted by a certain endpoint may not raise any privacy concerns on its own. However, gathering, collating, and analyzing even fragmented data from various endpoints might provide sensitive results. Nonetheless, in an increasingly interconnected world, manufacturers, developers, and end users must continue to strive for privacy protection within IoT platforms. With the number of connected devices directly linked to the Internet predicted to reach three times more by 2025, the potential for a rise in personal privacy concerns is evident. The study hypothetically suggests that promoting awareness and providing training and education to IoT users on information privacy protection will allow them to be more cautious when using IoT platforms or systems.

The study opted for online surveys in the form of questionnaires as a data gathering technique for IoT users. To respond to such questions, the responder must submit his or her opinion or point of view based on the research topic under study. Unlike other data gathering approaches, online surveys offer a larger reach, allowing many individuals to submit high-quality, trustworthy, and important data. The author created an artifact for IoT users to go through before attempting the real IoT privacy-related questions to educate them. In the next section, existing literature on privacy in IoT contexts is examined. The remaining sections deal with the problem statement, study aim, scope, and research questions. Some parts of the study also address the research techniques used in this study as well as the analytic strategy. Lastly, the final sections discuss the study limitations and future research prospects.

The study conducted for this research forms part of an honors research project module, HRCOS82 (Honours Research Report). HRCOS82 is a compulsory module for the Bachelor of Science Honours degree offered by the University of South Africa (UNISA). The objective of this research module is to prepare students for a postgraduate research study at a master's level. Students are afforded the prospect to pursue a research project with a view of producing a research report in a structured means under the supervision of study leaders within the School of Computing, UNISA. This research was conducted after obtaining ethical clearance from the designated research and university bodies that permitted the research to be conducted and reported on.

The organization of this research is mentioned as follows. The literature review of the existing works and their background information is provided in Section 2. Section 3 describes the research materials and methods. Section 4 elaborates the results and discussion along with the comparative analysis. Finally, the conclusion is stated in Section 5.

2. Related Work

2.1. Background of Privacy and Information Privacy. Despite numerous attempts to define privacy, no universal definition of privacy has been developed. Amid the fact that the right to privacy is universal, its concrete manifestation varies depending on the prevailing societal characteristics, as well as the economic and cultural environment [7]. That is, privacy must be reinterpreted in light of the current era and examined in its current context. Several factors influence what people consider private. There are significant differences between societies and cultures, and scientific advancement can also result in a different, pressing need for privacy protection [8]. It depends on the situation, on the context, as sharing the same information in different situations could be viewed separately.

Individual plays a significant role in which privacy can be thought of as a sort of "aura" that surrounds the individual and serves as a barrier between him/her and the outside world [9]. The limits of this aura change from context to context and from individual to individual, so an average standard must be found from all of these individualized and changing contexts, and this standard can be legally protected. Apart from this ever-changing context, numerous attempts to define privacy have been made over the last decade [10]. One of the best definitions of privacy is provided by Máté Dániel Szabó, a Hungarian jurist, who stated that "Privacy is the right of the individual to decide about himself/herself."

The idea of information privacy is a subset of the larger concept of privacy, which has been researched and debated for centuries. According to Quan-Haase and Ho [11], most interpretations of the idea of privacy allude to a human right, although in different settings. Mutimukwe et al. [12] identified four levels of privacy based on these contexts: (i) personal privacy, (ii) personal conduct privacy, (iii) personal communication privacy, and (iv) personal data privacy. Personal communication privacy and data privacy may now be integrated into the concept of information privacy since most conversations are digitized and preserved as information.

The study focuses on information privacy because it is the subject of the majority of privacy-related IS research [13]. This sole focus is unsurprising given that technology is generating many issues and some answers around data privacy. With the advancement of modern information and communication technology, data can be gathered, aggregated, and analyzed at a quicker and higher volume than ever before. Furthermore, data might be obtained without the consent of individuals. There are different definitions of information privacy, but the features of the definitions are quite consistent and often include some type of control over the potential secondary uses of one's personal information [13].

The process of employing data for reasons other than those for which it was initially obtained is referred to as secondary usage. Lamba [3] defines four aspects of information privacy: acquisition, unlawful secondary use, unauthorized access, and mistakes. Another taxonomy covers data gathering, data processing, data distribution, and invasion. Özkan [14] offers a taxonomy of information privacy in collaborative contexts based on time, matter, and space dimensions. The space dimension reflects a structural perspective of information privacy that incorporates individual, group, and organizational privacy.

Information privacy is simply defined as the protection of an individual's personal information [15]. Information privacy has turned out to be the most critical concern in today's digital age. If people are completely unaware of their privacy, the disclosure of personal information in digital communication settings may result in significant privacy issues in the future [16]. Even though people have a theoretical interest in maintaining their privacy when using the Internet and do not want everyone to know their personal data and confidential information, promoting information protection awareness can provide more insight for users on how they can manage their personal information. Privacy will be protected thanks to modern technology. People are irritated when they believe they have certain privacy rights but then learn that they do not [17]. We need to communicate with individuals so that they are aware of the problem ahead of time. Computer technology is not leading us into some terrifying new period that we will not be able to comprehend [18].

Quan-Haase and Ho [11] define information privacy as "an individual's interest in controlling, or at least considerably influencing, the processing of data about oneself." The term privacy is related to various ideas, definitions, and interpretations within the field of Information Systems (IS). Maram et al. [19] define privacy as "the desire of individuals to possess the liberty of choice no matter the conditions or amount to which they reveal their attitude and conduct to others." Lamba [3] defines privacy as "the management of transactions between people, with the last word objective of promoting autonomy and/or decreasing vulnerability." On the other hand, privacy is an individual's ability to manage information about themselves. They are distinct difference between privacy and security which is discussed in the following section.

2.2. Difference between Privacy and Security. Privacy and security are two different but connected concepts [11].

(I) Privacy is concerned with the usage and control of personal data, such as establishing policies to guarantee individuals' personal information is gathered, shared, and utilized in appropriate ways [20].

(II) Security is primarily concerned with safeguarding data from malicious assaults and profiteering from stolen data [21].

2.3. Background of the Internet of Things. We are witnessing the start of a brand-new age of the Internet of Things (IoT, also referred to as the Internet of Objects). The Internet of Things (IoT) is the networked interconnectivity of common items, many of which have all-knowing intelligence. The Internet of Things (IoT) will broaden the industry's scope by

incorporating every object enabling communication via embedded systems, resulting in a widely dispersed network of devices interacting with people and other devices [22]. In recent decades, the exponential rise of the IoT in the realm of computers has encouraged innovation and customized services that have improved people's living standards [23].

IoT devices are employed in a variety of industries, including manufacturing, engineering, computers, and small companies. Smart gadgets can investigate the surroundings, communicate with other intelligent items, and interact with people, allowing users to perform things more differently [24]. Because of fast developments in the underlying technology, IoT is enabling a plethora of unique applications that promise to improve the quality of our lives. In recent years, the IoT has piqued the curiosity of scholars and practitioners all around the world.

IoT has gotten a lot of academic interest in the last decade. IoT is viewed as a factor of the forthcoming Internet and will comprise billions of intelligent communicating things. The Internet of the future will indeed be composed of disparately linked devices that will gradually increase the borders of the world utilizing physical and digital components. IoT will provide new capabilities to link things. While the concept of the Internet of Things has been around for a long time, the latest improvements in a range of diverse technologies have made it a reality. The following technologies have made IoT feasible:

(I) Access to low-cost, low-power sensor technologies. Because of the availability of low-cost, trustworthy sensors, more firms can utilize IoT technology.

(II) Communication: A plethora of Internet network protocols have made it easier to link sensors to the cloud and other devices for efficient data transfer.

(III) Cloud computing platforms: with the expanded availability of cloud platforms, both organizations and consumers may now access the infrastructure they need to scale up without having to manage it all.

(IV) Analytics and machine learning are two of the foremost important aspects of machine learning. Businesses may gain insights more quickly and simply thanks to advances in machine learning and analytics, similarly to access to varied and vast amounts of knowledge stored remotely.

(V) Machine learning (AI): natural-language processing (NLP) has been supplied to the Internet of Things such as personal digital assistants Alexa, Cortana, and Siri through advances in neural networks, enabling them accessible, inexpensive, and feasible for home usage.

IoT is employed by automobile owners to remotely operate their cars, like preheating the car before the driving force gets in it or hailing a car through a phone [25]. Due to IoT's ability to enable device-to-device communication, cars will soon be able to schedule their own service appointments. Figure 1 gives an insight detail of IoT architecture:

2.4. Privacy in the Internet of Things. IoT provides users with a strong technical background and management over how to carry out ordinary duties by blanketing the environment with smart items [27]. Smart objects are slightly different computer devices such as embedded systems, sensor systems, and actuators which can disseminate and share data to facilitate positive interactions and rational choice creation in the Internet of Things [28]. Things are embedded in consumer devices and industrial machinery to collect and transmit environmental data. Smart objects can also cause physical changes in their environment and be controlled locally or remotely via the Internet. The privacy concerns addressed in the study which are applied to every IoT user are illustrated with examples that are related to smart appliances which are connected to devices. Further, the rate at which the users of smart devices are developed is out spaced by the rate that is protective for obtaining solutions that protect the information with the help of technologies. Despite the abundance of the Internet of Things and its impact on our daily lives, we must fully understand the threats and challenges they pose to our privacy.

2.5. IoT Privacy Challenges. Data gathering technologies in the IoT ecosystem have resulted in new privacy problems. Obtaining consent for data collection is one of these problems, as allowing users to manage, personalize, and choose the data they provide, and ensuring that the use of such data is confined to the stated purpose. These issues are exacerbated by the increasing risk of personal information misuse in the IoT sphere [13]. This is due to the widespread tracking of habits, actions, and whereabouts throughout time. IoT technologies bring new dangers to personal safety. The development of the digital computer has allowed the advance of some fields like statistics, while IoT has enhanced communication, information exchange, and collecting [29].

Yet, the data is present with a gigantic scale that is stored, sorted, and analyzed with the help of the government and large companies. Therefore, the capabilities support the data to gather deliberately the observation as surveillance and novel applications are offered by using the data acquired which is freely supplied for other purposes [30]. However, the effectiveness and reduced cost of data storage enable the long-term preservation of massive volumes of potentially illegal material [31]. A representation or information string associated with a person's identity cannot be deleted or forgotten, whether on the public Internet or in classified data storage.

Another privacy challenge raised by IoT is the difficulty in establishing safe and secure communication. This is due to the fact that the technology consists of various components at the network edge, making it difficult to ensure that all of the components communicate safely and securely. There are also some concerns about data secrecy and confidentiality associated with IoT. The technology, for example, entails the interconnection of multiple networks, whereas in most cases, a user may not have control over some networks, exposing data to numerous secrecy and confidentiality threats.

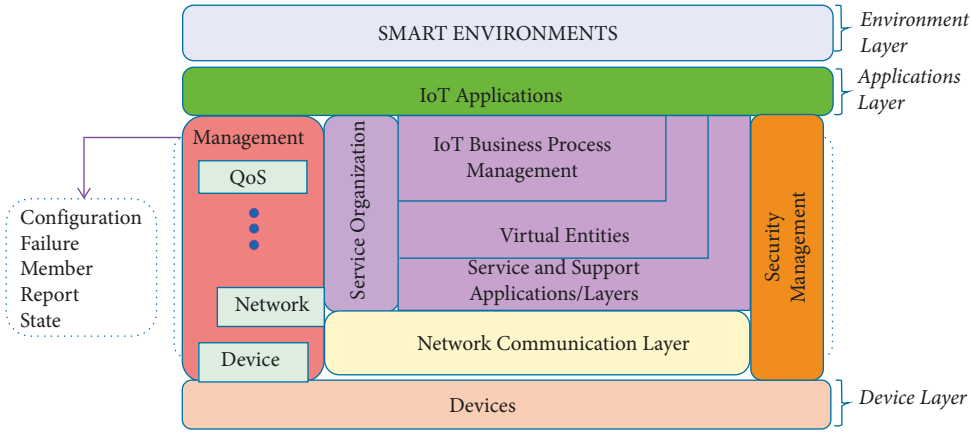

Figure 1: Internet of Things reference architecture (IoT-RA) [26].

Furthermore, IoT involves a large number of devices and networks. This makes identifying, assessing, and monitoring critical components to ensure compliance with privacy policies difficult [32]. However, it is difficult to ensure an adequate level of secure information exchange and trust between various vertical information technology infrastructures. Other IoT privacy issues are discussed below in detail:

(I) Identification, Localizing, and Tracking.

The evolving features and technologies of the Internet of Things, as well as the emerging systems of IoT interaction, have resulted in specific privacy challenges. One of the IoT's privacy challenges is identifying the risk of associating an identifier, such as an address, with the individual and related data [33]. The main challenge, in this case, is associating the identity with a specific context, which violates the individual's privacy by providing identifying information to entities outside the user's personal sphere, thereby increasing the potential cyberattack vectors.

(II) Profiling and Authentication.

The Internet of Things also poses significant privacy challenges in terms of profiling, interaction, and presentation, all of which violate privacy. In terms of profiling, the Internet of Things poses a risk in the collection of data about users in order to determine their interests through correlation with other data and profiles [34]. In this case, profiling methods in e-commerce may be used for consumer personalization as well as internal targeting and optimization based on customers' interests and demographics. Profiling, on the other hand, can lead to privacy violations if data is used for unsolicited advertising, price discrimination, and social engineering.

(III) Lifecycle Transitions and Inventory Attacks.

IoT raises concerns about privacy due to lifecycle transitions and inventory attacks. In this case, the users' confidential information gathered during the lifetime of the IoT device may be revealed during changes to the gadget's control spheres during their lifecycle [35]. The smart devices interact with a wide range of services and people, accumulating data on such interactions in their history logs. Given that the lifecycle of most consumer goods is based on the customer owning the products in perpetuity, the sale or sharing of such devices could result in the buyer gaining access to sensitive data about the previous owner, infringing on the individual's privacy.

The next section delivers a comprehensive summary of the privacy measures in the IoT context that emphasizes more on protecting individual personal information.

2.6. Information Privacy Protection Measures in IoT. Traditional Internet privacy concerns mostly affect connected persons using the Internet. However, in IoT contexts, privacy problems may affect persons who are not utilizing any IoT services but are present in the surroundings [36]. Internet apps may employ well-established authentication mechanisms to record data flow, evaluate any privacy infractions, and promptly warn the user. However, due to the lack of well-defined control domain boundaries in IoT contexts, it is significantly more difficult to properly catch privacy infractions. As a result, IoT settings must respect individuals' privacy and ensure that personal data acquired is utilized for just the intended purpose. Finally, obtained data should be kept for as long as it is necessary. Table 1 lists necessary measures that can be applied in IoT privacy protection:

3. Materials and Methods

3.1. Introduction. This section indicates the methods used to discourse the focal research question and achieve the objectives indicated in the preceding sections. The research onion in Figure 2 illustrates the study methodological approach that leads to the development of a concrete research

Table 1: Possible privacy-preserving strategies in IoT contexts.

References	Measure	Summary
[37]	Authentication and authorization	Mechanisms for lightweight authentication and key establishment
[38]	Privacy awareness	Informs customers about confidential information gathering, risks involved, and how to utilize IoT services responsibly and prevent personal information from leaking
[37]	Data encryption secure channel using IPSec	Ensures secure data interchange and information delivery. The IPSec protocol provides authentication as well as encryption. Demonstrates a 6LoWPAN/IPsec extension for IoT device security
[39]	2FA (Two-factor authentication)	Double authentication using SMS codes and e-mail to authenticate

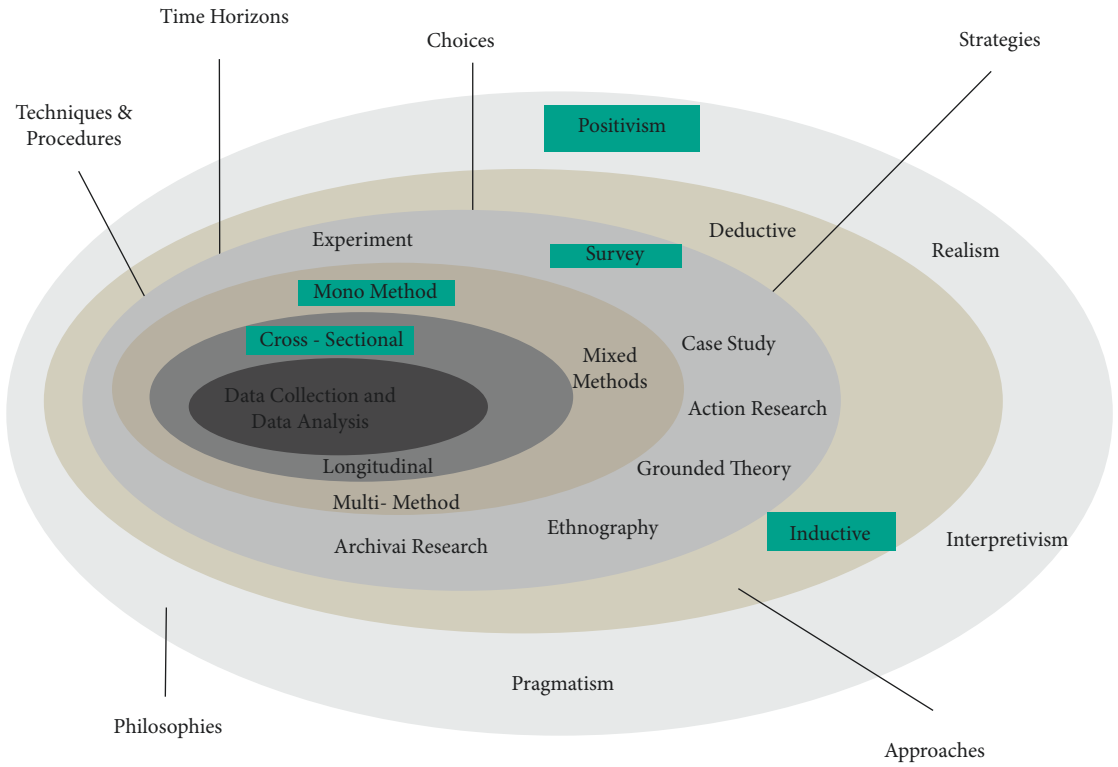

Figure 2: The research onion [40].

theory by addressing each critical stage involved in the process.

3.2. Research Philosophy. Research philosophy is about different beliefs about the nature of the topic under study. Research philosophy is subdivided into three groups: Ontology, Epistemology, and Axiology [41]. Epistemology is widely used in scientific research since it aids in locating the information that can be demonstrated without a question; in other words, it aims to identify universal acceptable knowledge and manage the facts properly [42]. Philosophical viewpoints within the epistemological worldview include positivism, pragmatism, realism, and interpretivism. Positivism is there to generate research topics and hypotheses that may be tested and examined [43]. It can also be used to quantify and explain common knowledge about the study under investigation which is why this study opted for the positivism approach.

3.3. Research Method. The research onion contains other two essential elements which are deductive and inductive. Within positivism methods, data is evaluated first, important patterns are accustomed to inform the generation of findings, and the inductive approach may be employed successfully. In contrast to the deductive approach, the inductive strategy allows one to create their own theory rather than employing one that already exists. The inductive approach is characterized by a move from the precise to the broad, which is why this study opted for it [44].

3.4. Research Strategy. A range of techniques, like experimental research, action research, case study research, interviews, survey, and scientific literature review, are often utilized according to the nature of the research. This study opted for an open-ended survey and questionnaires. Surveys are one of the foremost effective and cost-effective research strategies. This data gathering technique most often delivers

Table 2: Age group breakdown.

Variable	Frequency	Percentage (%)
1970–1985	8	21.6
1986–1994	13	35.1
1995–1999	5	13.5
2000–2021	11	29.7
Total	37	100

enough accurate data to the author based on the topic under study. Surveys are typically employed, and they entail sampling of the community on which the study is focused [45]. It enables the collection of massive amounts of information that will be utilized to answer generated research questions.

3.5. Data Collection and Analysis. A descriptive method was used to analyze the results of this study. Online questionnaires were applied as a way of collecting data from users on their views and concerns about information privacy protection. Online questionnaires are easier to conduct and give a quick means to get replies and are a straightforward way to process data. Also, because one of the study's requirements was that a person is an IoT user, the use of an online questionnaire survey was satisfactory. Finally, this study used an online questionnaire survey to meet the study's objectives, which were to assess IoT user awareness and concerns about information privacy and protection, as well as to identify any common attitudes and differences.

4. Results and Discussion

The purpose of this quantitative study is to promote information privacy awareness among IoT users and identify privacy risks based on data collected from them through a survey. To successfully validate this research, the data collected was analyzed to provide answers to the main research question: "What percentage of IoT users are knowledgeable/aware of data protection and privacy?". Data is interpreted descriptively, as described earlier in the previous section. The online survey was completed by 97.6% of participants, with the remaining 2.4% declining to participate. Data gathered from the survey was subjected to frequency counts. In other words, the participants' responses to each individual question were added up to get the maximum frequency of occurrence or the number of times a certain response occurred. Some questionnaire findings are offered in the form of tables and charts for greater accuracy and comprehension.

4.1. Demographic Information. Table 2 shows all participants' age group information. The study's target age range was between 20 and 35 years old, and 78.3% of participants fell into this category.

According to the data gathered, 50% of the population were male, 47.5% were female, and 2.5% preferred not to say. The survey's qualification breakdown revealed that 46.2% of participants held grade 12 qualifications, 7.7% were diploma candidates, 28.2% held three-year university degrees, 10.3% held honors degrees, and 7.7% did not have any of the above-mentioned qualifications. According to the study, 55% of the participants were employed, while 45% were unemployed.

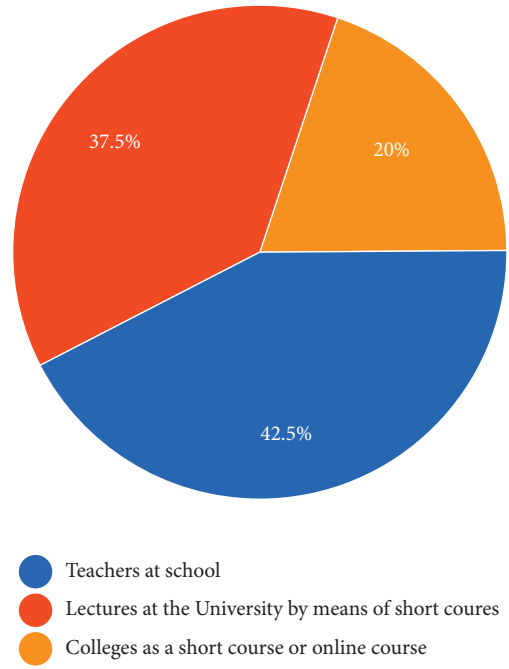

Figure 3: IPP training breakdown.

4.2. Information Privacy Protection Awareness Status in IoT Context. Around 47.5% of the respondents had previously touched on the subject of privacy and threats related to information privacy protection, while 52.5% were unaware of any threats or dangers linked with IPP. Participants rated their understanding of information privacy protection as follows: 12.5% had no awareness, 10% had poor awareness, 45% had average awareness, 22.5% had good awareness, and 10% had a strong understanding. Data protection, cloud privacy, IoT privacy, and POPIA (Protection of Personal Information Act) were some of the significant privacy protection topics identified during the course of data gathering. 35% of participants admitted to being victims of a data breach, whereas 65% had never encountered such a scenario. Most participants stated that information privacy protection is required within the community to educate, raise awareness, eliminate human error, and enable individuals to be conscious of their privacy when browsing the web.

4.3. Education/Training. As indicated in Figure 3, the majority of participants consented to be trained on information privacy protection awareness. Approximately 42.5% of responders strongly believe that IPP training should be taught in school by teachers while 37.5% of participants, on the other hand, stated that training should be done via lectures at universities in the form of short courses. Only 20% suggested IPP training be offered at colleges as a short or online course. Figure 3 shows the precise age highlighted to begin teaching

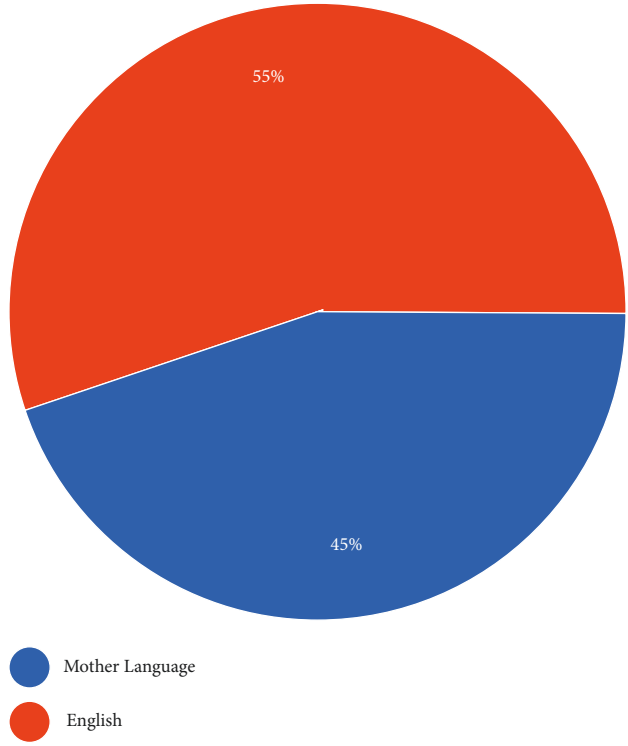

Figure 4: IPP preferred training language.

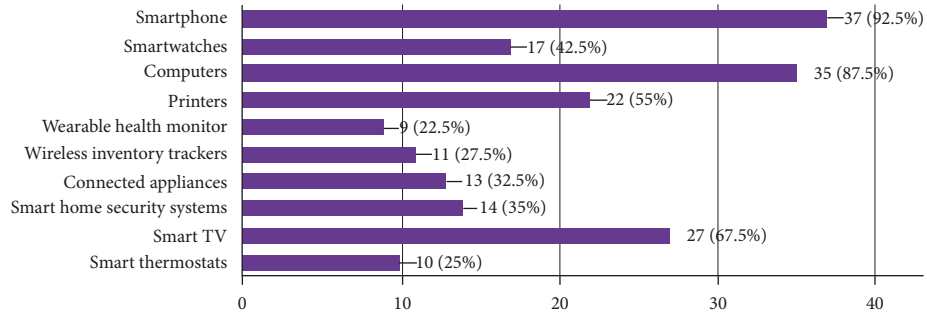

Figure 5: Internet-connected devices.

individuals about information privacy protection, and the majority of responses from participants suggested training between the ages of 15 and 18 years. In Figure 4, the majority of the participants (55%) agreed that information privacy protection material should be offered in English, while 45% believed it would be more effective if the content would be presented in the participant's native tongue. On the same point, 75% of participants agreed to be informed about IPP using online awareness materials, while 22% preferred workshops.

4.4. Information Privacy Protection Awareness Artifact Evaluation. Following a thorough review of the artifact, 81.6% of the participants strongly agreed to have learned a lot about information privacy protection in the context of IoT, with just 18.4% responding not to have grasped the concept adequately. 87.5% of participants indicated that the artifact was well presented and informative about IPP, whereas 12.5% did not find it very informative. 30.8% of participants agreed that by 2022, about 26.5 billion gadgets are expected to be connected to the Internet of Things. Figure 5 depicts the most often utilized Internet-connected gadgets by participants. Smartphones are the most often used Internet-connected devices, with a 92.5% rating.

Approximately 97.5% of participants found the IoT privacy guidelines presented in the artifact to be extremely valuable and agreed to implement these suggestions in the future to preserve their privacy in an IoT environment. Following the examination of the artifact, 62.5% of the participants were able to employ end-to-end encryption when sending their data, while 37.5% were unable to do so. Figure 6 depicts the number of participants who are aware of the IoT risks if they do not comply with the privacy

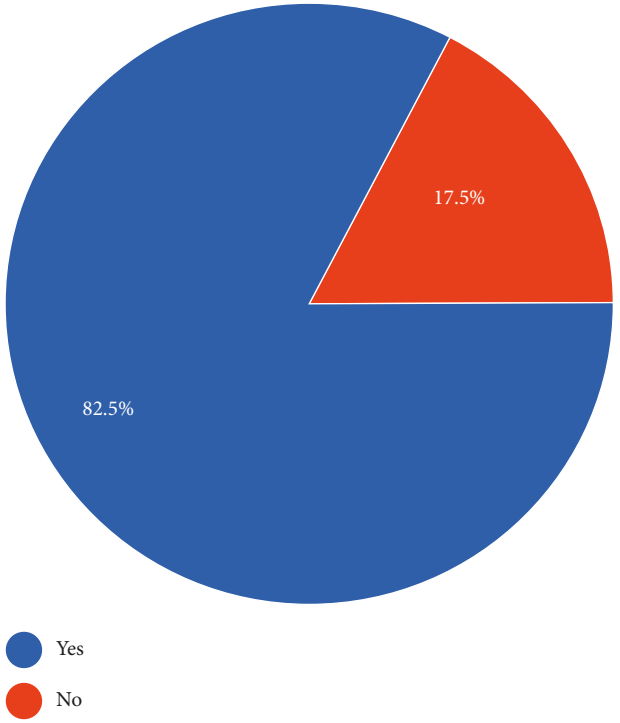

Figure 6: IoT harms.

principles indicated in the artifact. Those who were aware of IoT risks/harms responded with a Yes, while those who were not aware of any IoT-related risks responded with a No.

After complete artifact evaluation, the majority of participants (90%) were aware and educated of several IoT privacy preservation methods including two-factor authentication, or 2FA, which is an extra layer of protection used to safeguard the security of IoT accounts.

4.5. Discussion. Participants' ratings of their awareness of information privacy protection turned out to be average, suggesting a need for education and awareness. Approximately 42.5% of responders strongly believe that IPP training should be taught in school by teachers. Individuals should be taught information privacy protection between the ages of 15 and 18 years old, according to the agreed-upon age range by responders. Most participants (55%) agreed that information privacy protection content should be offered in English. 35% of those respondents admitted to being victims of a data breach. Smartphones were the most often utilized Internet-connected devices, with a 92.5% rating. Approximately 97.5% of participants found the IoT privacy guidelines presented in the artifact to be extremely valuable and agreed to implement these suggestions in the future to preserve their privacy in an IoT environment. Several participants stated that information privacy protection is required within the community to educate, raise awareness, eliminate human error, and enable individuals to be conscious of their privacy when surfing the Internet. After the participant's evaluation of the artifact, 81.6% of the participants strongly believed that they were knowledgeable on information privacy protection in the context of IoT. Participants rate the artifact as well presented and informative. Finally, most participants' comments on the IoT privacy artifact presented to them as a means of educating and increasing awareness were extremely positive, which made the artifact an effective method of spreading/sharing information privacy protection awareness to IoT users.

5. Conclusion

Individual privacy protection is a major challenge in this digital era. We contribute to a better understanding of how individuals' knowledge of privacy risks affects their privacy-related actions by concentrating on the conceptualization of IPA. Individuals might be concerned about their privacy, but the so-called privacy paradox shows that they do not behave in line with their stated views. It is therefore mandatory in this digital era to always enhance people's understanding of the need of protecting their privacy and know the ethical use of IoT platforms. Privacy may also be misinterpreted, yet it has the capacity to encourage criminality and exploitation of systems, while secretive connections between terrorists could endanger safety. As a result, privacy is not a universal virtue. Instead, philosophical and legal research must be conducted into the realms of privacy, the substance of privacy, and the advantages and damages that privacy protection may create to find the conditions under which privacy is valued enough to sustain the maintenance of private rights. However, individuals can protect their Internet privacy in several ways. Protective measures are specific computer-based actions that users desire to safeguard their information. People can protect their online privacy by limiting the knowledge they reveal and setting up place privacy protections. Furthermore, knowledge, talents, and skill all play a task. People that have higher Internet skills, technological experience, and understanding of the IoT are more likely to interact with privacy protection measures. Boosting information privacy awareness will have an enormous impact in helping individuals to be completely alert to the risks and ethical procedures they must take into consideration to safeguard their personal information. In that instance, the study went above and beyond in examining the level of alertness posed by individuals when making use of IoT systems or platforms. The study contributed more to individuals' awareness by improving their knowledge level of information privacy protection through online questionnaires and artifacts that reflect the measures and steps that need to be adhered to when dealing with interconnected smart technologies. The paper enhanced individual understanding of privacy-related issues that need to be recognized when dealing with IoT platforms or systems. After a complete evaluation of the study results, the artifact presented provided the majority of individuals with adequate knowledge that will enable them to safeguard their personal information. The rapid growth of IoT platforms and systems will continue to bring more issues related to individual privacy. As such privacy cannot be fully mitigated especially with the amount of data exchanged hourly, daily, or weekly, instead it can be controlled and more awareness needs to be promoted. Therefore, it is wise for individuals to

have adequate knowledge and advanced awareness of how they can protect themselves from any sort of privacy-related threats before their systems get exposed to IoT attacks.

Data Availability

The data used to support the findings of this study can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Miguel Garcia-Torres would like to thank the Spanish Ministry of Science, Innovation and Universities for the support, under project PID2020-117954RB-C21, and the Junta de Andalucía, for projects PY20-00870 and UPO-13851.

References

[1] H.-T. Chen, "Revisiting the privacy paradox on social media with an extended privacy calculus model: the effect of privacy concerns, privacy self-efficacy, and social capital on privacy management," *American Behavioral Scientist*, vol. 62, no. 10, pp. 1392–1412, 2018.

[2] C. Y. Yoon, "Measurement of smart technology capability for manufacturing fields in a smart technology environment," *International Journal of Information and Electronics Engineering*, vol. 9, no. 3, pp. 67–71, 2019.

[3] A. Lamba, "A through analysis on protecting cyber threats and attacks on CPS embedded subsystems," *International Journal of Current Engineering and Scientific Research*, vol. 1, no. 3, pp. 48–55, 2014.

[4] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of things (IoT): smart and secure service delivery," *ACM Transactions on Internet Technology*, vol. 16, no. 4, pp. 1–7, 2016.

[5] A. Harit, A. Ezzati, and R. Elharti, "Internet of things security: challenges and perspectives," in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, Article ID 167, Cambridge, UK, March 2017.

[6] P. Menard and G. J. Bott, "Analyzing IoT Users' Mobile Device Privacy Concerns: Extracting Privacy Permissions Using a Disclosure Experiment," *Computers & Security*, vol. 95, Article ID 101856, 2020.

[7] A. J. Bidgoly, H. J. Bidgoly, and Z. Arezoumand, "Towards a universal and privacy preserving EEG-based authentication system," *Scientific Reports*, vol. 12, no. 1, Article ID 2531, 2022.

[8] R. Al-Asbahi, "Structural anonymity for privacy protection in social network," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 11, no. 6, pp. 102–107, 2021.

[9] M. Becker, "Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy," *Ethics and Information Technology*, vol. 21, no. 4, pp. 307–317, 2019.

[10] A. McIver, T. Rabehaja, R. Wen, and C. Morgan, "Privacy in elections: how small is 'small,'" *Journal of Information Security and Applications*, vol. 36, pp. 112–126, 2017.

[11] A. Quan-Haase and D. Ho, "Online privacy concerns and privacy protection strategies among older adults in East York, Canada," *Journal of the Association for Information Science and Technology*, vol. 71, no. 9, pp. 1089–1102, 2020.

[12] C. Mutimukwe, E. Kolkowska, and A. Grönlund, "Information privacy in e-service: effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior," *Government Information Quarterly*, vol. 37, no. 1, Article ID 101413, 2020.

[13] F. Alshohoumi and M. Sarrab, "Privacy concerns in IoT A deeper insight into privacy concerns in IoT based healthcare," *International Journal of Computing and Digital Systems*, vol. 9, no. 3, pp. 399–418, 2020.

[14] E. Özkan, "Why do consumers behave differently in personal information disclosure and self-disclosure? The role of personality traits and privacy concern," *Alphanumeric Journal*, vol. 6, no. 2, pp. 257–276, 2018.

[15] D. K. Mulligan, C. Koopman, and N. Doty, "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy," *Philosophical Transactions of the Royal Society A: Mathematical, Physical & Engineering Sciences*, vol. 374, no. 2083, Article ID 20160118, 2016.

[16] K. Degirmenci, "Mobile users' information privacy concerns and the role of app permission requests," *International Journal of Information Management*, vol. 50, pp. 261–272, 2020.

[17] S. Peisert, "Some experiences in developing security technology that actually get used," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 4–7, 2019.

[18] S. Barth, M. D. T. De Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and Informatics*, vol. 41, pp. 55–69, 2019.

[19] B. Maram, J. M. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for UNICODE data privacy and security in IOT," *Service Oriented Computing and Applications*, vol. 13, no. 1, pp. 3–15, 2019.

[20] Y. Meier, J. Schäwel, and N. C. Krämer, "Between protection and disclosure: applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites," *Studies in Communication and Media*, vol. 10, no. 3, pp. 283–306, 2021.

[21] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[22] C. Wu, Y. Zhang, and Y. Deng, "Toward fast and distributed computation migration system for edge computing in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10041–10052, 2019.

[23] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "Internet of things: security in the keys," in *Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '16)*, pp. 129–133, Malta Malta, November 2016.

[24] U. L. Tupe, S. D. Babar, S. P. Kadam, and P. N. Mahalle, "Research perspective on energy-efficient protocols in IoT," *International Journal of Pervasive Computing and Communications*, 2021.

[25] P. Prasant, S. Bhardwaj, M. Gupta, M. Srivastava, J. Singh, and R. K. Maurya, "Role of internet of things in protecting different wearable gadgets and materials," *Materials Today Proceedings*, vol. 56, pp. 3387–3393, 2022.

[26] J. de C. Silva, J. J. P. C. Rodrigues, J. Al-Muhtadi, R. A. L. Rabêlo, and V. Furtado, "Management platforms and

protocols for internet of things: a survey," *Sensors*, vol. 19, no. 3, Article ID 676, 2019.
[27] C. Li and B. Palanisamy, "Reversible spatio-temporal perturbation for protecting location privacy," *Computer Communications*, vol. 135, pp. 16–27, 2019.
[28] N. Bugshan, I. Khalil, N. Moustafa, and M. S. Rahman, "Privacy-preserving microservices in industrial internet of things driven smart applications," *IEEE Internet of Things Journal*, p. 1, 2021.
[29] A. Bashir and A. Hussain Mir, "Securing communication in MQTT enabled internet of things with lightweight security protocol," *EAI Endorsed Transactions on Internet of Things*, vol. 3, no. 12, Article ID 154390, 2018.
[30] S.-H. Sim and Y.-S. Jeong, "Multi-blockchain-based IoT data processing techniques to ensure the integrity of IoT data in AIoT edge computing environments," *Sensors*, vol. 21, no. 10, Article ID 3515, 2021.
[31] A. Pandia, "Aadhaar infringing fundamental rights," *SSRN Electronic Journal*, 2018.
[32] F. Amato, V. Casola, G. Cozzolino, A. De Benedictis, and F. Moscato, "Exploiting workflow languages and semantics for validation of security policies in IoT composite services," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4655–4665, 2020.
[33] L. Atzori, C. Campolo, B. Da et al., "Enhancing identifier/locator splitting through social internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2974–2985, 2019.
[34] B. Mbarek, M. Ge, and T. Pitner, "An efficient mutual authentication scheme for internet of things," *Internet of Things*, vol. 9, Article ID 100160, 2020.
[35] J. Wang and J. Liu, "Deep learning for securing software-defined industrial internet of things: attacks and countermeasures," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 11179–11189, 2022.
[36] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of things (IoT): a review," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 521–526, 2021.
[37] M. Tanveer, G. Abbas, Z. H. Abbas, M. Waqas, F. Muhammad, and S. Kim, "S6AE: securing 6LoWPAN using authenticated encryption scheme," *Sensors*, vol. 20, no. 9, Article ID 2707, 2020.
[38] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, Article ID 4102, 2020.
[39] S. Certic, "Two-factor Authentication vulnerabilities," *SSRN Electronic Journal*, 2018.
[40] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, Financial Times Prentice Hall, Hoboken, NJ, USA, 2007.
[41] S. B. Andrade and D. Andersen, "Digital story grammar: a quantitative methodology for narrative analysis," *International Journal of Social Research Methodology*, vol. 23, no. 4, pp. 405–421, 2020.
[42] B. Poopuu, "Dialogical research design: practising ethical, useful and safe(r) research," *Social Epistemology*, vol. 34, no. 1, pp. 31–42, 2020.
[43] S. Tüzemen, "Advances in modern physics: transition from positivism to post-positivism in education and research," *Advances in Research*, vol. 6, no. 1, pp. 1–9, 2016.
[44] A. Bryman and E. Bell, *Business Research Methods*, Oxford University Press, Oxford, England, 3rd edition, 2011.
[45] J. Bibb, "Publisher's note," *Surveys in Operations Research and Management Science*, vol. 21, no. 2, p. 135, 2016.