Received: 24 January 2024 | Revised: 10 October 2024 | Accepted: 28 October 2024 | Published online: 8 May 2025

RESEARCH ARTICLE

Artificial Intelligence and Applications
2025, Vol. 00(00) 1–15
DOI: 10.47852/bonviewAIA52022523

BON VIEW PUBLISHING

Ground Theory Based Empirical Analysis of Security Issues and Challenges Associated with Internet of Things

Sangeetha S. K. B.[1], Sandeep Kumar Mathivanan[2], Saurav Mallik[3,4,*] and Hong Qin[5,*]

[1]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, India*

[2]*School of Computer Science and Engineering, Galgotias University, India*

[3]*Department of Environmental Health, Harvard T H Chan School of Public Health, USA*

[4]*Department of Pharmacology & Toxicology, The University of Arizona, USA*

[5]*Department of Computer Science and Engineering, University of Tennessee at Chattanooga, USA*

Abstract: Using the Internet and its interconnected technologies, people and equipment will be able to communicate not just in real time but also at anytime and anywhere. Therefore, it is impossible to ignore the myriad risks associated with such rapidly evolving technology or their effects on almost everything. The study's goal is to gain a better understanding of how the Internet of Things functions and, most importantly, what security, privacy, and trust issues are associated with it, moreover, what factors people need to think about when purchasing, using, and disposing of such devices. A thorough analysis is carried out to understand privacy and security problems regarding IoT devices and people's opinions of them. The collected data are analyzed using fundamental theory, and the responses are categorized to find several themes. The findings indicated that technical interest, comfort, and cost savings are people's top priorities for smart IoT devices. Important conclusions are reached, and understanding the underlying theory makes people more familiar with common sense when it comes to security and privacy concerns with IoT devices. The findings showed how much people knew about IoT device risks in proportion to their age and level of technology interest. Young people are happier and more conscious than grownups. Other suggestions for the acquisition, use, and disposal of IoT devices are also presented.

Keywords: grounded theory, Internet of Things, IoT components, security, threats, privacy, focus group

1. Introduction

IoT, or the Internet of things (IoT), is a network that connects various electronic gadgets, mechanical and digital machines, objects, animals, and even humans, all of which are assigned their own unique identifiers and can exchange data with one another in real time and without any need for human intervention. Numerous modern household gadgets and appliances have Internet connectivity, can be monitored, and can be remotely controlled via apps on smartphones. The IoT is this predicament. Smart home gadgets and services that interact automatically and in real time make up IoT surroundings [1, 2]. It is a potent technical advancement that not only changes the lives of common people but also the way that businesses, governments, and industries operate on a worldwide scale. Making ordinary people's life more pleasant is the primary goal of consumer IoT [3, 4].

Despite the fact that the IoT benefits people, communities, and businesses, the status of smart cities and intelligent countries will be the focus of its future effects. At the municipal level, information and data from residences, communities, buildings, and institutions are merged for improved power management, traffic management, and city planning, enhancing the advantages for the general public [5, 6]. The same is true for business and industry, where we can improve customer service and expertise, automate supply and production chains, fully use goods and services, and manage performance effectively and efficiently. Aside from these advantages, there are problems about security dangers, privacy invasions, and trust issues with smart gadgets [7].

Protection, identification, and monitoring of hazards, as well as assistance in fixing vulnerabilities from a variety of devices that can offer security concerns to the organization, are all part of the process of safeguarding the IoT from threats and breaches. Similar to voice commands, smart assistants carry the risk of potential data breaches by responding to voice instructions and sending data over the Internet. Such information about presence or absence from the home could potentially compromise security and privacy if it falls into the wrong hands. Issues are also brought up by the environment and the volume of data that smart devices collect before sending it to service providers. Who will use it, how will it be used, and who will have access to it? by yet another indicator of

*Corresponding authors: Saurav Mallik, Department of Environmental Health, Harvard T H Chan School of Public Health and Department of Pharmacology & Toxicology, The University of Arizona, USA. Email: smallik@pharmacy.arizona.edu and Hong Qin, Department of Computer Science and Engineering, University of Tennessee at Chattanooga, USA. Email: hong-qin@utc.edu a significant query. Each new smart gadget may pose a new security risk if they are not treated appropriately throughout their lifespans [8].

Integrated technology has become an essential component of consumers' personal lives due to the development of smart home technology and its diversity of usage. Due to the lack of regulation around the production of IoT devices and the vast amounts of data that pass through them, we are continuously at risk of being attacked online. The increased necessity for IoT security solutions is a direct result of the hazards associated with using IoT devices. In recent years, researchers have become interested in the outcomes. Studies specifically looked at issues with privacy and security, public opinion, understanding of people, and hurdles to the adoption of smart home technologies. To give people a greater understanding of the issue, what should be considered while purchasing, using, and discarding these devices, as well as their top safety and privacy concerns [9]. The study also aims to provide the usual, inexperienced reader with an overview of the IoT, and it is concerned by the people. Based on the discussion, the main purpose of this study is to examine the following questions:

1) What concerns about security, privacy, and trust arise with IoT devices?
2) How well-versed and concerned are individuals with security, privacy, and security in relation to IoT devices?
3) What aspects should consumers take into account when purchasing and utilizing IoT devices?

The research stated above makes contributions by drawing attention to the concealed and potentially harmful components of IoT devices and by educating the general public about cutting-edge technology like the IoT, which they use in a variety of ways. With this detailed introduction, Section 2 examines the background research on IoT, Section 3 outlines the research method, Section 4 outlines the assessment, and Section 5 outlines the findings and discussions followed by the conclusion in Section 6.

2. Motivation

The widespread use of IoT devices has transformed our interactions with technology by providing previously unheard-of levels of connectedness and convenience. It is impossible to ignore the numerous security, privacy, and trust issues that have arisen as a result of this quick expansion. It is becoming more and more clear as the IoT landscape develops how important it is to recognize and deal with these issues in order to protect user data, privacy, and general digital wellbeing.

The observed diversity and abundance of approaches available for addressing security and privacy issues within the IoT domain is a major driving force behind the proposal of this study. A plethora of techniques, strategies, and solutions have emerged to mitigate associated risks with the growing number of IoT devices and applications. But there are so many different approaches that it can confuse researchers, decision-makers, and end users, among other stakeholders.

This confusion is further compounded by the absence of standardized datasets, evaluation criteria, and measures. Researchers and practitioners may find it difficult to effectively compare and evaluate various methods in the absence of a cohesive framework. The size, complexity, and representativeness of the datasets used to assess IoT security and privacy solutions vary greatly, producing inconsistent findings and conclusions.

To make matters more complicated is the multiplicity of ideas and concepts in this field. Key terms like privacy, security, and trust may be interpreted differently by different researchers in the context of the IoT, leading to a fragmented understanding and inconsistent terminology usage. This discrepancy obstructs progress toward creating solid and workable solutions in addition to impeding communication and teamwork.

The numerous ways that IoT technology is being applied in various industries provide another incentive. IoT devices are widely used and have a wide range of applications, from smart homes and healthcare to industrial automation and transportation. Different application domains have different needs and challenges, so customized strategies and solutions are needed. On the other hand, the profusion of domain-specific solutions could mask more general insights and best practices that work in a variety of situations.

Given these reasons, a thorough survey or review is necessary to study that can provide insightful information about the state-of-the-art, point out areas that need more investigation and standardization, and direct future efforts toward creating reliable and comprehensive solutions for securing the IoT ecosystem by synthesizing and analyzing the literature that is currently available.

3. Related Study

A network of embedded sensors, software, and other associated technologies known as the IoT is designed expressly for transmitting data through the Internet. Simple domestic goods to cutting-edge commercial and industry products and technologies can be included in these gadgets. We are surrounded by intelligent objects that can talk to one another and add together. For instance, industrial equipment, high-end smartphones, home appliances, and light sensors. The IoT is an umbrella term for these many networks of these kinds of devices.

The IoT is a network that enables the connection of various things to the Internet at any time and from any location. It is currently regarded as one of Industry 4.0's most crucial technologies. The IoT market is expected to grow from $1.6 trillion to $14 trillion by 2025, having an impact on practically every sector of the economy and human health [10, 11]. This market's return on investment or income is also excellent. Data gathering and sharing verified this IoT feature, demonstrating its potential to communicate information across all platforms in an integrated framework and upgrading the common working image to enable new applications. This IoT capability is the communication of sensors and open devices [12, 13].

Building billions of wireless devices with the ability to communicate with anything and anybody will enable the IoT to realize its vision of revolutionizing the Internet. Increasing RFID processing capacity, multi-wireless network (WSN) networks, and low-cost storage are three strategies for achieving this, which will lead to the creation of a highly diverse resource network linked to a flexible network system [12, 14]. In actuality, IoT makes it feasible for communication not only between gadgets but also between people and their surroundings. The citizens, corporations, and government will all be significantly impacted by the IoT. Within the network, each IoT device must be separately visible [15, 16].

Data collection on devices uses a variety of sensory tools, including smart sensors, actuators, and RFID tags. Data from IoT devices are processed using calculations. Additionally, this procedure is utilized to get rid of extra or pointless data. Calculations on the gathered data can be done using a variety of computer hardware and software tools. Users receive services related to such device operations based on the data they receive. The most important feature of IoT devices is semantics. Describe how IoT devices may find precise information in their virtual locations and offer that information as a service [17].

As shown in Table 1, different IoT topologies have been introduced over time by various academics, and both academia

Table 1
Comparison analysis

Method	Concept	Objective	Datasets	Experiments	Challenges
Machine Learning-based Intrusion Detection Systems (IDS)	Utilizes ML algorithms to detect abnormal behavior and potential attacks in IoT networks.	Enhance IoT security by identifying and mitigating threats in real time.	NSL-KDD, CICIDS2017, IoT-23	Performance evaluation on detection accuracy, false positive rate, and computational efficiency.	Limited labeled datasets for training, adaptability to evolving attack patterns.
Blockchain-based Access Control	Utilizes blockchain technology to manage and enforce access control policies for IoT devices and data.	Ensure secure and immutable access control in distributed IoT environments.	Ethereum blockchain, Hyperledger Fabric	Simulation and testing of access control policies in blockchain networks.	Scalability, latency, consensus mechanisms, integration with existing IoT protocols.
Privacy-Preserving Data Aggregation	Employ cryptographic techniques to aggregate and anonymize IoT data while preserving privacy.	Protect user privacy while allowing for efficient data analysis and aggregation.	Private data generated from IoT sensors and simulations.	Evaluation of data utility, privacy preservation, and computational overhead.	Trade-off between privacy and utility, key management, scalability.
Federated Learning	Distributed machine learning model training across IoT devices to preserve data privacy.	Improve model accuracy without centralizing sensitive data.	MNIST dataset, CIFAR-10, IoT-generated data.	Assessment of model convergence, communication overhead, and privacy guarantees.	Heterogeneity of IoT devices, communication constraints, model synchronization.
Threat Intelligence Sharing Platforms	Facilitate the exchange of threat intelligence among IoT stakeholders.	Enhance collective defense capabilities and situational awareness.	Open source threat intelligence feeds and proprietary datasets.	Analysis of platform effectiveness in threat detection and response.	Trust establishment among participants, data validation, and integrity.
Hardware-based Security Solutions	Incorporates hardware security modules (HSMs) and trusted execution environments (TEEs) to protect IoT devices at the hardware level.	Provide robust protection against physical and logical attacks.	ARM TrustZone, Intel SGX platforms.	Evaluation of security features, performance impact, and resistance to tampering.	Cost, compatibility, complexity of integration with existing hardware designs.

and business have accepted them. IoT technology is made up of various interconnected technologies. Sensors, actuators, CPUs, and transceivers are the components of IoT devices. Devices that interact with their physical surroundings include sensors and actuators [18]. The data must then be carefully processed and kept in order to achieve the greatest outcomes from it. Additionally, these lines of communication are continually at risk from deceit, misrepresentation, and cyberattacks [19].

The study probably looks at qualitative aspects of responsible consumption with a particular emphasis on clothing. It might explore how customers feel about ethical and sustainable fashion industry practices, as well as their attitudes and behaviors in this regard [15]. It is likely that the study looks into the attitudes and actions of young consumers who choose to buy luxury goods that have been previously owned [1, 20]. The study might investigate what influences their decisions, how they feel about sustainability, and how they define luxury in relation to pre-owned items. It is anticipated that the study will address how artificial intelligence (AI) has affected marketing strategies. It may discuss different uses of AI in marketing strategies and evaluate how they affect companies and consumer behavior. Examples of these include predictive analytics, personalized advertising, and customer segmentation [16, 21].

The study investigates the variables influencing the purchasing behavior of millennials, with an emphasis on the function of influencer marketing. It might look into how millennials' brand preferences and purchase decisions are impacted by influencer partnerships and endorsements [22, 23]. The study explores how influencer marketing affects the purchasing habits of millennials. It may pinpoint the main causes of millennials' interaction with influencer content and the ensuing patterns of their purchases [24, 25]. Using the DEMATEL (Decision Making Trial and Evaluation Laboratory) approach, the study most likely offers a framework for assessing smartphone purchasing behavior in the Indian market. It may examine a number of variables that affect consumers' decisions, including features, pricing, brand perception, and technological advancements [26, 27].

The study most likely uses empirical research to examine the variables influencing consumer behavior in the fast-food sector. It might look at factors influencing consumers' decisions to consume fast food, such as affordability, taste, convenience, health consciousness, and cultural preferences [28]. The study addresses the opportunities and difficulties related to the digital transformation of marketing strategies. It might examine the challenges and dangers associated with this transformation process, as well as how data analytics, online platforms, and emerging technologies are reshaping business models, customer engagement, and marketing strategies [29, 30].

As a result, data analysis is carried out theoretically and emphasizes data patterns. Finally, guidelines for research standards, research boundaries, and ethical issues related to data gathering are also developed. Our study makes a unique contribution by specifically focusing on the privacy and security concerns related to the purchasing, usage, and disposal of IoT devices, which has been less explored in prior studies. While much of the existing research (e.g., [cite studies]) has focused on general privacy and security issues in IoT or technical vulnerabilities in IoT systems, our work specifically addresses consumer behavior and how individual perceptions of security and privacy risks affect decision-making throughout the lifecycle of IoT devices [23, 25]. This human-centric approach provides new insights into how people of different age groups and technical interest levels perceive and respond to IoT device risks [27, 31, 32].

In contrast to previous works, which focus on the technical aspects of IoT security (e.g., encryption, secure communication protocols), our study shifts the focus towards the social and psychological aspects of IoT usage [33]. By examining factors like comfort, cost savings, and technical interest alongside privacy and security concerns, we provide a more holistic view of how consumers interact with IoT devices [34, 35]. Our findings show that younger users are generally more aware of security risks and more comfortable using IoT devices compared to older adults, a trend that has not been thoroughly examined in prior studies. These insights could help shape future guidelines for both consumers and manufacturers regarding the safe use and disposal of IoT devices.

4. Research Methodology

4.1. Research paradigm & methodology

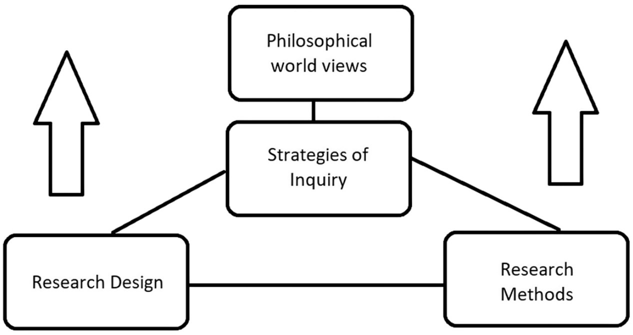
The study is based on three major paradigms for truth: positivist, interpretivist, and critical. The paradigms guide the scientific inquiry approach in terms of intellectual frameworks that develop from structuring ontology (the nature of reality) and epistemology (the nature of knowledge). Of these, interpretivism is closely related to qualitative research, which forms the core of the proposed methodology. Interpretivism lays emphasis on the importance of understanding the truth, because it is socially constructed, whereby a person derives meaning from his interactions and notions in a contextual framework. This is again directly associated with epistemology because the former very simply seeks to interpret meaning rather than dig out objective facts, and ontology assumes that truth is a social artifact [31, 36–38].

The research design integrates these paradigms by structuring the study into several key phases, beginning with formulating the research questions and selecting appropriate methodologies. The study follows an idiographic research strategy, emphasizing the detailed examination of specific events or participants' experiences within the research context, in this case, a live event at the university. This approach is effective for resolving research issues by focusing on context-specific insights rather than generalizable laws.

The research design as shown in Figure 1 employs five different methodologies:

1) Surveys
2) Questionnaires
3) Archives
4) Histories
5) Case studies

Figure 1
Framework for research design



These methodologies are used to gather qualitative data. The questionnaire is specifically designed with open-ended and exploratory questions to elicit detailed responses, allowing participants to express their perspectives freely. This aids in generating rich, interpretive data that supports the interpretivist paradigm.

4.2. Research strategy

The research strategy begins by describing the research questions and methodologies, followed by outlining the study plan and relevant information systems domains. Given the dynamic nature of data collection during a live event, the study adheres to a flexible research strategy, allowing iterative refinement of the research plan. The use of idiographic research strategy is particularly suited for examining the perspectives of participants within this specific event, which contributes to the interpretivist nature of the research [39].

4.3. Research approach

The research follows three core methodologies of study: experimental, descriptive, and non-descriptive. The research widely employs an experimental method within the translation research paradigm since it explains matters that are better suited to a specific class of people. This has mainly made it practicable for the study to research matters of complexity of issues, scope, possible solutions, and essential matters that are supposed to be dealt with throughout the course of the investigation. This method of experimentation incorporates methods applied in qualitative research, which collects in-depth data through comprehensive interviews and observations along with detailed case studies. In addition, an exploratory approach is adopted in conducting research in the problem. This approach allows for the flexible investigation of the bigger, systemic concerns as well as the specific, detailed aspects of the phenomenon under study [22, 40].

4.4. Data collection & data collection methods

There were 240 study participants in all. There are 240 participants, 132 men, and 108 women. There were 102 individuals aged 20 to 25, 76 aged 25 to 30, 42 aged 30 to 35, and 20 each aged 35 to 45 and 45 to 55. Over the course of two to three weeks in the month of March 2022, data are gathered and examined. The sample is chosen for a predefined or predetermined purpose throughout high-quality research projects. Additionally, the sample chosen is consistent with the goals and issues of the research that is being done. IoT devices are likely to be present in the homes of participants. The data are collected as follows in Table 2.

4.5. Open-ended survey

Open-ended questionnaires were used for collecting data due to the nature of study's objectives. The questions are rather scripted and prepared, despite being open-ended. An online survey with open-ended questions is the first stage in gathering empirical data from the target population, which is chosen from LinkedIn. Question categories include departure, exploratory, and engagement. The purpose of the study is to collect information on the main topic and respondents to determine how much the target audience is aware of the IoT, its uses, limitations, and potential threats. Answering open-ended questions with a simple "yes" or "no" is not acceptable.

4.6. Procedure

Step 1: Personal preferences, such as political affiliation, dress code, or religion, are not the subject of any sensitive or provocative questions.

Step 2: Firmly grasp the environment.

Step 3: Since respondents are the primary information sources, it is crucial to choose respondents who are knowledgeable, open to participate, and familiar with the neighborhood.

Step 4: To clearly understand their level of subject-matter expertise and what people of various ages think about IoT technology.

Step 5: The crucial stage of survey execution is gaining respondents' trust.

Step 6: Memos and notes can be used to collect data.

Descriptive statistics would first provide an overview of the sample's features and enable comparisons between various groups by summarizing the responses. A comparative analysis would go farther, determining whether responses from different demographic groups or at different stages of technology adoption differ significantly from one another. Relationships between variables, such as the relationship between security concerns and willingness to pay for upgraded features, may be found through correlation analysis. In order to find predictors of particular outcomes, regression analysis would investigate the factors that influence attitudes or behaviors in more detail.

4.7. Focus groups

Focus groups are a well-liked high-quality research technique in which a small group of people are questioned about their opinions, attitudes, and perceptions about a certain good, service, concept, or area of the economy. This activity offers crucial insight into the participants' motivations and interests. The procedure of choosing participants and respondents is the first and most crucial step in

Table 2
Survey questions

Objective	Data collection methodology
What concerns about security, privacy, and trust arise with IoT devices?	The definition and explanation of IoT systems, their design, underlying technology, and operation are built upon a review of the literature. The objective is to identify the main security and privacy threats related to IoT devices and technology.
How well-versed and concerned are individuals with security, privacy, and security in relation to IoT devices?	Examined through responses from a focus group with the intended audience on LinkedIn
What aspects should consumers take into account when purchasing and utilizing IoT devices?	Investigated using trustworthy web sources were looked at to identify the best solution.

carrying out a focus group study. The selection of participants and respondents received careful consideration by the researcher. 125 respondents in total took part in the data collection process.

The goal is to identify solutions to security and privacy problems that affect people of all ages in order to better grasp the situation. The oldest respondents are between the ages of 55 and 60, and the youngest respondents ranged in age from 30 to 35. There are a maximum of 30–32 items on the questionnaire. Engagement questions are used at the beginning to introduce the attendees. The next section switches to more "test questions" "so you can see what kinds of IoT devices they are using, how familiar they are with them, how much they are assisting them in their daily life, and so on. They are aware of their security and privacy. "Exit queries" are used to close the session to make sure that we did not have any important details that would help analyze the data over time.

4.8. Data analysis

In order to draw new conclusions from the data and to draw attention to recurrent themes in order to comprehend what the data is saying, I apply a grounded theory with an inductive method.

4.9. Grounded theory

Because grounded theory is both a process and an outcome, applying it to actual facts as opposed to considering it as a theory will help us better grasp how it functions and how to draw insightful conclusions from it. This study does not address the security and privacy concerns related to IoT and smart devices. In novel research areas, grounded theory is frequently utilized to analyze socio-technical activities and technological advancements. The information that needs to be evaluated therefore may be qualitative, quantitative, or both.

4.10. Queries

1) What is your name, whereabouts, contact information, and address?
2) How intriguing do you find modern technology, smart houses, and smart gadgets?
3) What attributes of smart home technologies do you use or prefer?
4) Do you understand the risks that smart gadgets represent to your security and privacy?
5) How often do you change the router and smart device passwords?
6) Are you willing to give your information to outside parties in exchange for extra offers and discounts?
7) What steps should firms take to produce products that are more dependable and safe?

Studies that focus on what occurs, how people communicate, and how they understand are usually concerned with social processes or behaviors. Grounded theory research begins with open-ended inquiries about the respondents' personal information and general attitude toward technology, which is the same approach I used in my interviews.

4.11. Ethical approvals

The information gathered is employed in theory capture's initial and subsequent sampling. A fundamental theory needs to be coded. Coding serves as a crucial link between the collection of data and the growing theory used to interpret it. The objective of this phase is to preserve as much coded information as possible. Following the focus group's opening questions, a wealth of information—including the respondents' personal particulars, their level of technical knowledge, their degree of technological caution, and their knowledge of security and privacy—is accessible through the first codes.

It focuses on assessing the study's internal and external validity while adhering to the guidelines for exploratory research. Internal validity is solely relevant to the study at hand because it is used to determine how well participants understand the IoT devices they use. Internal validity is the process of establishing links between the study's variables. The information for the study report is compiled using both primary and secondary sources.

1) What goal does this data gathering serve? (in response to researchers' questions about IoT usage and security/privacy),
2) When was the information gathered?
3) How was the information gathered? and whether the data agrees with that found in other sources?

Let's now discuss external validity, or how broadly research findings may be applied to various contexts, populations, locales, and measurements. In quantitative research, the capacity to exactly replicate the techniques and outcomes is referred to as a reliability test.

4.12. Limitations of the study

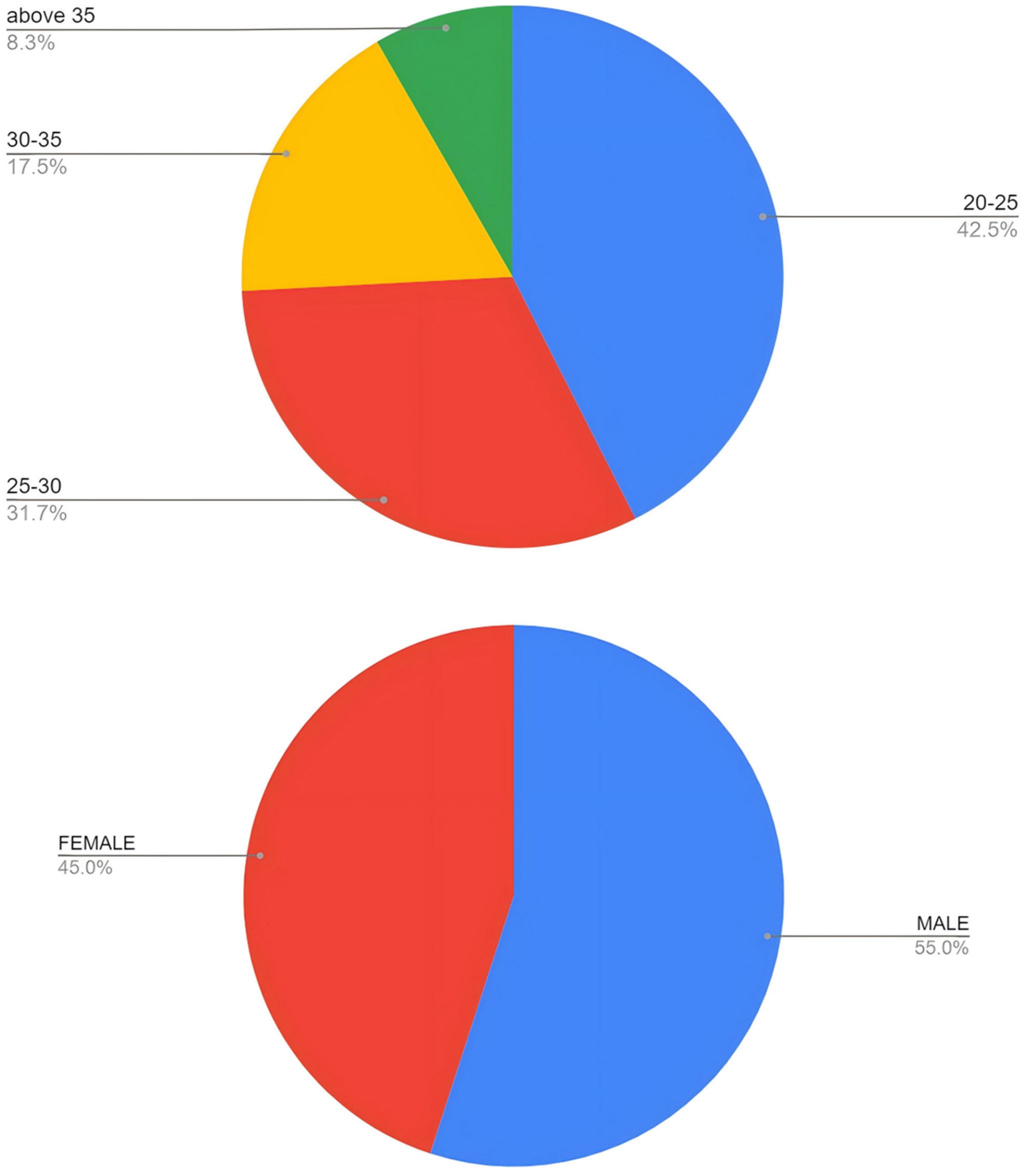
Another issue is the need for a particular set of abilities while collecting, compiling, organizing, and interpreting qualitative data. Additionally, since descriptive information and data are more commonly used than numerical or statistical information, producing the outcome demands more focus and work. The goal is to prevent or minimize these problems since "design defects" can cause a cascade of errors that ultimately threaten the legitimacy and dependability of the entire research process. Finally, people might not have been interested in sharing their thoughts at that time because stress and anxiety levels are higher than usual due to the COVID-19 Pandemic, the lockdown, and other safeguards put in place. A sincere effort is made to protect privacy. Wherever people are mentioned, their names are not used; instead, responders 1, 2, and so on are used to refer to them. Considering that privacy and security are the study's main points, maintaining personal data is an important part of the analysis. The consent form template, which is made as a Google form, is provided to the respondents.

5. Experimentation Analysis

A pre-selected set of respondents participates in focus groups and surveys that are done concurrently. Each respondent is asked a total of 18 questions, and each one's answers are recorded and examined. Respondents are encouraged to cross-communicate with one another in order to support the focus group session. Surveys are taken during a focus group with 240 LinkedIn respondents to determine the general public's awareness of, comprehension of, involvement with, and projected adoption of IoT technology.

The total number of study participants is 240, as depicted in Figure 2. Among the 240 participants, 132 of them are men and 108 of them are women. There were 102 individuals aged 20 to 25, 76 aged 25 to 30, 42 aged 30 to 35, and 20 each aged 35 to 45 and 45 to 55. In March 2022, data will be gathered and examined for a few weeks. 176 of the 240 respondents expressed a strong interest in utilizing technology in their daily lives and household appliances. It is clear that because they are between the ages of 20 and 30, young people are more interested in cutting-edge technology and gadgets. While the two adult responses are completely uninterested, the 14 middle-aged participants are

Figure 2
Respondents' analysis



theoretically interested but aren't all that joyful or excited about it. Figure 3 depicts the usage analysis.

Nearly everyone had not heard of the terms "smart homes" and "smart home gadgets," with the exception of one elderly woman who had heard of nor had any interest in technology. The knowledge analysis is displayed in Figure 4. All respondents know about smart systems because they are a feature of their recently constructed homes. 202 respondents are aware of virtual assistants like Alexa, Google Assistant, and others. The existence of intelligent virtual assistants is unknown to 38 people. 167 poll respondents are familiar with smart homes. Then there are smart appliances for the house, including TVs, fridges, vacuums, and music players. Quite a few people also brought up intelligent agriculture. 192 people are aware of the connections between smartphones and automobiles.

Figure 5 demonstrates how younger age groups have more technology and devices at home than older age groups do. An average of three gadgets and devices are used daily by those between the ages of 30 and 40. Even though some of the older and middle-aged respondents owned routers and other technology, many lacked IT skills. The respondents used a variety of virtual tools. With three responders apiece, Google Assistant and Amazon's Alexa are found to be the most widely used virtual assistants. Both Microsoft's Cortana and Samsung's Bixby were disliked by the respondents.

Participants are questioned about their use of IoT devices and smart home equipment as well as what level of comfort and functionality they expected, as shown in Figure 6. The answers varied greatly, indicating the injured people's age range. Most participants thought listening to music was enjoyable. The use of smartwatches has the second-most popular application. The topic of home security also piqued the participants' curiosity. Approximately 224 out of the 240 participants reported either home security or remote home security at the top level. They are drawn to smartphone apps that could be used to control remote Wi-Fi cameras, smart home alarms, and smart door locks. Many members also track their fitness and health using the proper technology.

Figure 3
Gadgets usage analysis

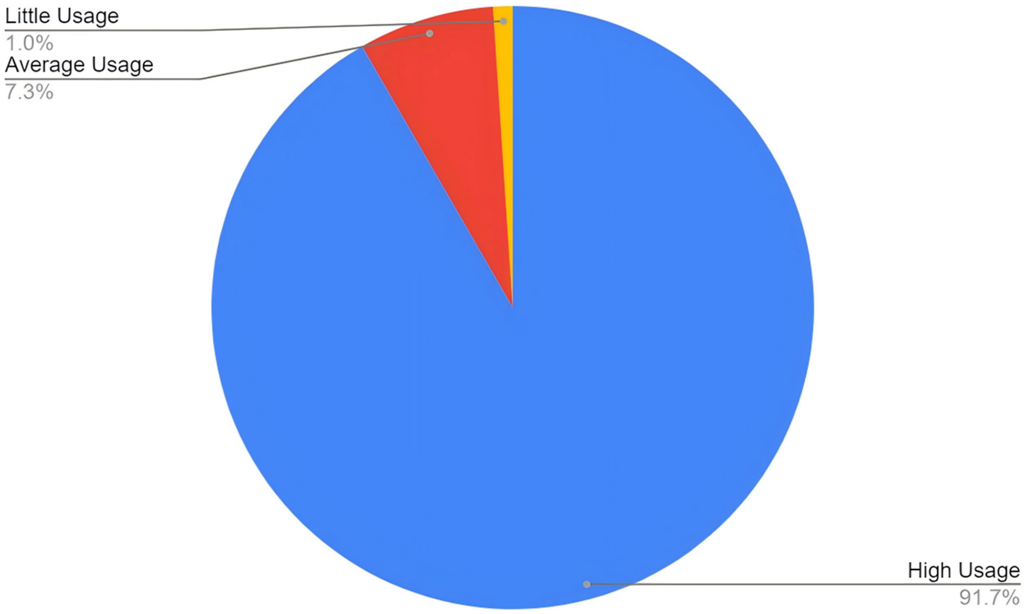
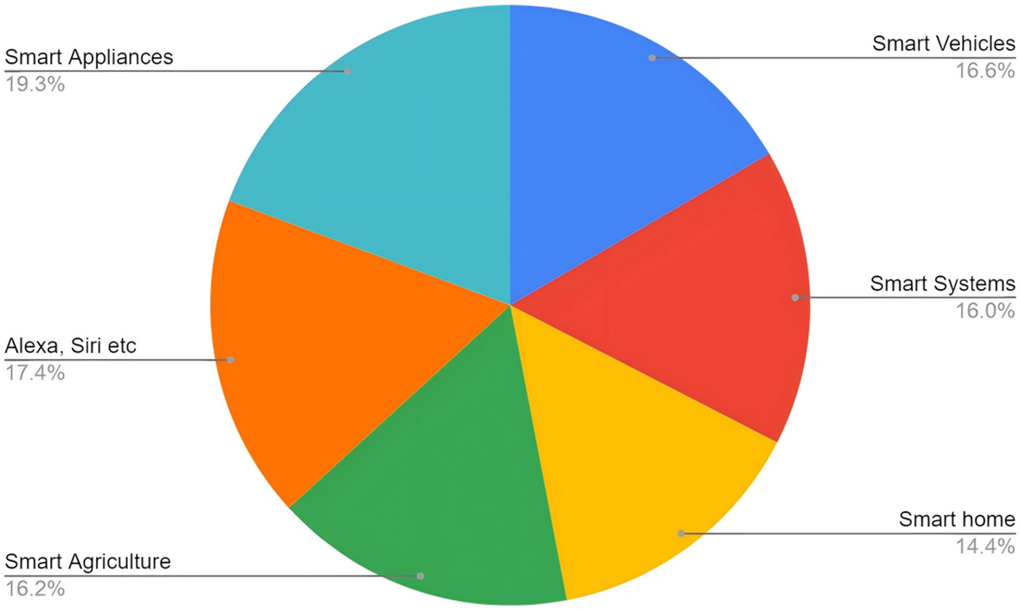


Figure 4
Smart systems knowledge analysis



The 240 responders are all router owners. These routers come in a variety of varieties. Primarily employing high-speed routers with a 1000 MBPS speed cap. The majority of responders used "spaced networks." Surprisingly, individuals in their middle age or older also used them. But they also admitted that they used family members as a resource to build networks. When informed of the equipment or themselves, 216 out of 240 respondents indicated they routinely updated their router settings. 24 respondents are regular reviewers, yet the majority of them are middle-aged or older. The explanation is not acceptable because they are unable to do so or found it challenging to constantly remember their passwords. Participants are unaware of the effects, particularly those in their 40s and 60s. Purchasing reason analysis is depicted in Table 3.

In Table 3, the response to the question about the motivation for the purchase is crucial for figuring out the general attitudes and behaviors of the respondents as well as what motivated them to purchase these IoT or smart gadgets. Participants are questioned about who motivated them to purchase IoT devices as well as how much marketing and advertising influenced their choice. In response, friends and family have been the key drivers of smart

Figure 5
No of gadgets usage analysis (%)

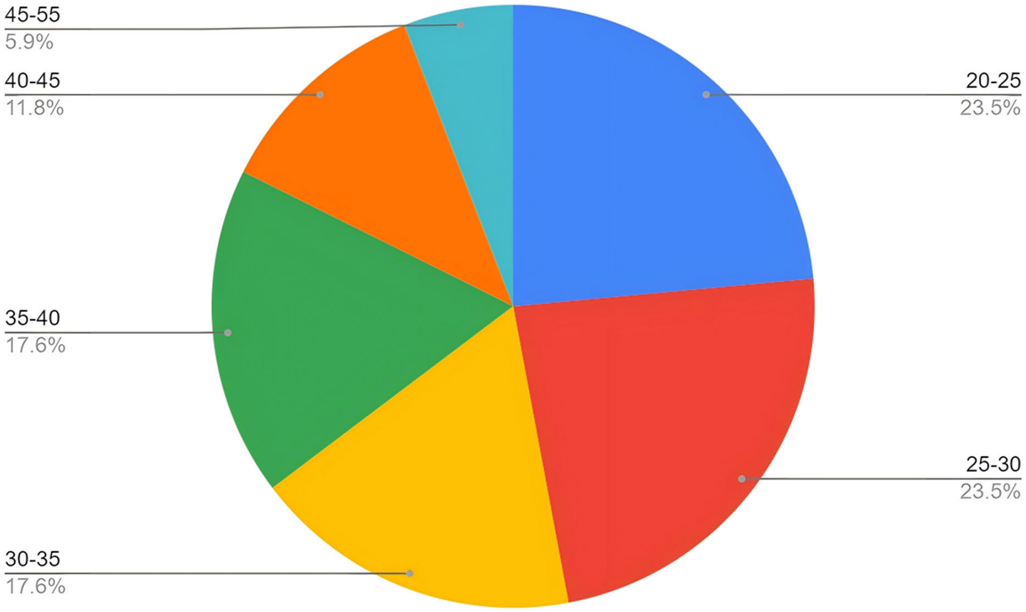


Figure 6
IoT services usage analysis

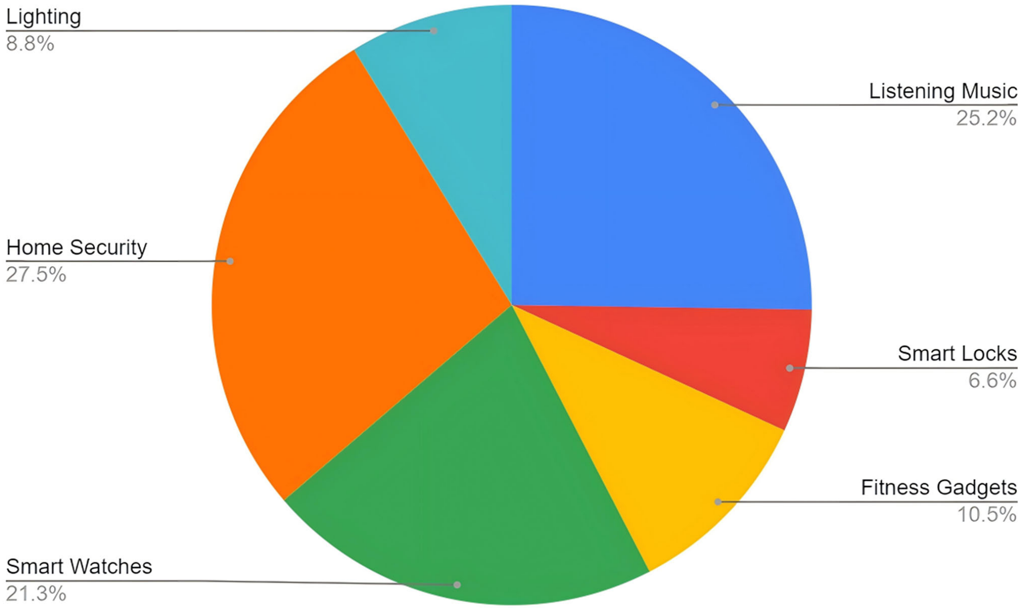
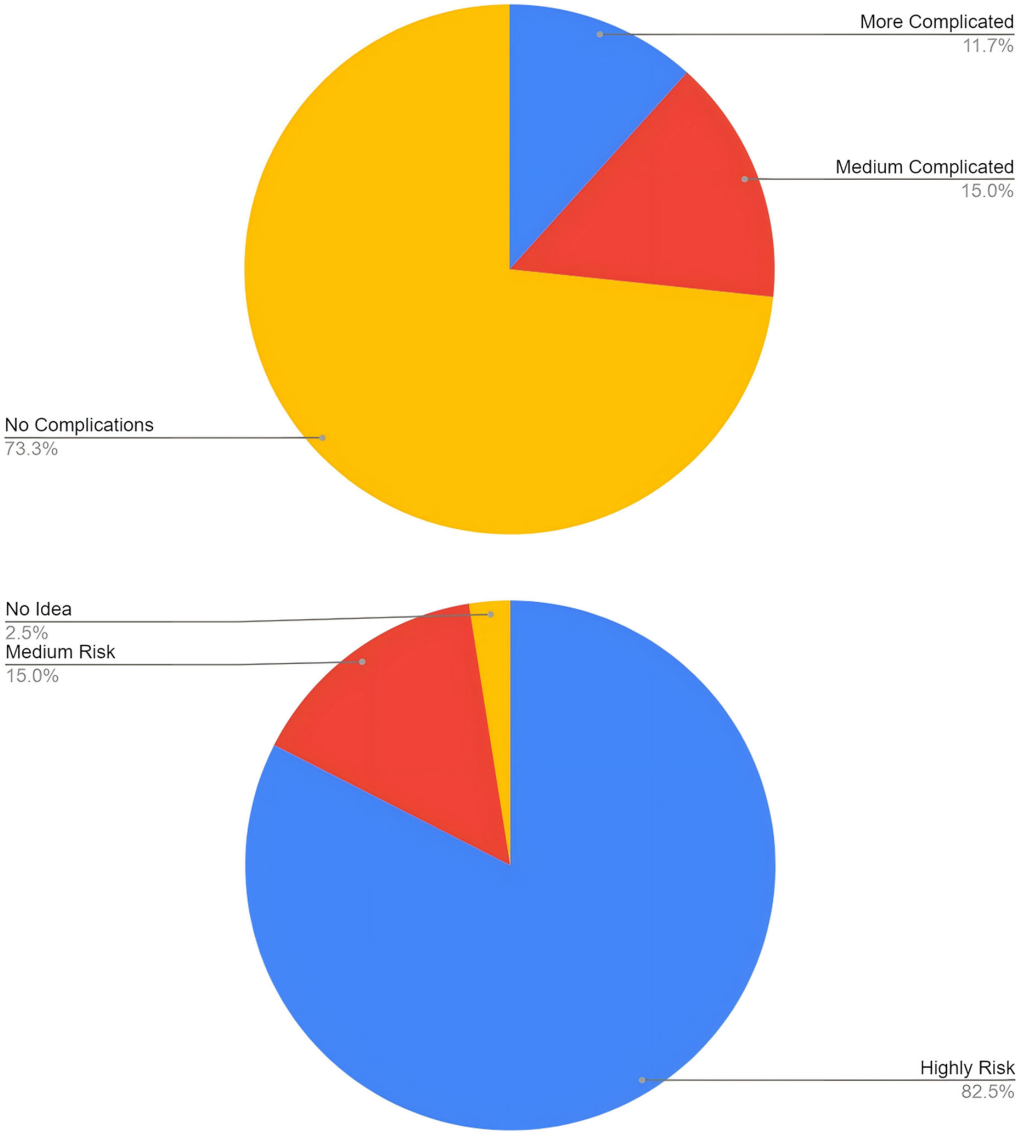


Table 3
Purchasing reason analysis

No	Reason to purchase IoT devices
1	To control home appliances
2	To make an alarm
3	To follow healthy lifestyle
4	To reduce expenses and bills
5	To bring comfort
6	To get modern look
7	To follow trend

home device purchases. Many participants, who ranged in age from 40 to 50, reported that members of their immediate families already used smart home equipment and described the advantages and conveniences of utilizing them on a regular basis. But they are also pressured by marketing and advertising on various social media websites, like Facebook, Instagram, Twitter, YouTube, and blogs, to consider buying or using these devices. Nearly all of the participants indicated that they occasionally, whether deliberately or unknowingly, click on social networking sites. advertisements for smart home appliances, and they leave cookies on that website or forum to remember their preferences. They finally kept being

Figure 7
Complications in usage analysis



attacked with the same ads, too. They were ultimately forced to buy this equipment as a result of this as shown in Figure 7.

1) Respondent 7 (25–30 years old): "A close family member compelled me to make a smart purchase."
2) Respondent 9 (aged 30–35): "I received it as a present to improve my quality of life."
3) Respondent 8 (35–40 yrs.) "I always see advertisements on my Facebook wall."
4) Respondent 2 (aged 40 to 45) and 4 (aged 35 to 40) both stated, "I got good recommendations from my friends," "Social media impacted me a lot, nearly forced me," "TV advertising made me buy one," and "weekly ads magazine made my decision," as I frequently read that magazine.
5) Respondent 4 (45–50 years old): "I was not impacted by these items; not much was in my flat when I moved in.

Following suit, reasons for selecting smart home technologies included upgrades from older systems and built-in smart features in homes. Additionally, 28 participants claimed that it is impossible to ignore the influence of technology and that social media has opened up new channels for them to communicate with different product manufacturers and businesses, which help them make decisions. According to 28 out of 10 respondents, these IoT devices are more challenging to use. These 28 people ranged in age. 146 said they are easy to use and understand. The majority of them are in their 30s to 40s. They are quite easy to use, according to 78 respondents, the majority of whom worked in the IT industry.

36 individuals are aware that smart or IoT devices carry risks, but they are unsure of the specific types of risks. (Theft of identities, theft of private data, theft of financial data, or another crime). The 48 persons are more aware of the threats, but they are still lacking the entire picture. 6 aren't even aware of it, though. Participants are generally aware of the privacy and security concerns related to IoT devices. However, many are unsure whether these tools or the incorrect individuals could utilize these devices to invade their privacy. Additionally, they might steal their private information, like likes and dislikes, daily schedules, and financial and other sensitive data. 25–28 participants, on average, in the 30–50 age range.

The elder individuals, between the ages of 50 and 60, are largely oblivious of the danger. They had no idea that thieves or criminals could utilize their information and data because every linked item to their home sent digital fingerprints wherever it went, displaying the matching activity on smartphones when it is used. Additionally, cybercriminals who examine their addiction can find out about their daily routine and watch their films, images, or maps of their homes in case they commit another crime in the future. Participants who are aware of the burglary while discussing privacy and security issues using terms like identity theft, online burglary, and information in the wrong hands may try to control it. But aside from that, they have never expressed a significant concern about using the device.

Participants also expressed concern over the collection of voice and image data, anonymous recording, social media use, access to financial information, and the storage, transmission, and use of their personal data by gadgets without their consent. Concerns included credit card information, location (such as whether a person is at home or not, when they arrive or go), and medical and health information.

Apart from the above analysis Table 4 depicts the list of questions used for more detailed analysis.

Participants drew a fine line between privacy and data security and allowed some types of data. One speaker used the example of intelligent lighting to show how data collection is a common commercial activity. It is difficult to predict how long the light will endure in the absence of data. In this case, it was appropriate for you to gather data, but not when the maker of the gadget intended to sell it or use it for specialized advertising. The comments indicate that there is a distinct difference between data collection and privacy breach. The participants desired greater luxury, but greater luxury would compromise their privacy or identity; therefore, they are not ignored.

Five people didn't regularly update their smart device passwords. Only three did, and only two of them are serious about it. The 46 respondents used unique passwords on several machines, but as it is challenging to remember multiple passwords at once, they used the "password vaults" offered by various businesses to save all of their credentials in one location. To enter that location, they each used the same password. 126 individuals, including adults, shared the same password across all of their devices. 65 people either never reviewed the product or only did so when it was absolutely necessary. Some features, according to them, are free, do not function, or start to display error messages if they are not updated as ordered.

It is crucial that they can utilize these gadgets and navigate them because respondents indicated that they have varying abilities or understanding about technology and its application. Customer satisfaction came in second, so if something goes wrong or a customer is unable to use a product, there should be a helpful person at the help desk to aid them. The respondents also considered how their personal information will be used and maintained. They did not want it to be utilized for social media, email, or direct marketing. Additionally, respondents emphasized the significance of taking ethical standards into account when marketing products. There shouldn't be any unstated terms and conditions involved.

Table 4
More survey questions

No	Question
1	Have you ever been hacked?
2	Have you read the privacy policy?
3	Have you accidentally downloaded malware?
4	Have you accepted the purchase agreement ?
5	Have you given more personal data for offerings?
6	Are you changing passwords more often?
7	Do you use the same passwords for all logins?
8	Do you update versions often?
9	Are you satisfied with the device's usage?

The majority of survey participants expressed general satisfaction with the smart home appliances they utilized, particularly the smart controller, smart lighting, and visual aids. The other defendant is not happy because it is challenging for him to work for himself. They remained neutral in their experience, nevertheless. Data collecting for service improvement but sharing of personal information with outside parties. Large corporations like Facebook, Microsoft, and Google are fully aware of your identity. Does Alexa record everything I say for Amazon to use? Do we know more about ourselves than Google does? 225 out of the 240 participants voiced this worry. These responses demonstrate that participants are aware that it is the duty of device manufacturers to protect user privacy and data.

Participants that purchased and used smart home/IoT devices emphasized their effectiveness, lower utility costs, luxury, convenience, intelligence, real assistants, home alarms, and ability to customize lighting as needed. Overall, respondents expressed complete satisfaction with the goods and services received, regardless of how usability or performance had changed. Additionally, according to respondents, this is where the future is. However, they had concerns about the device manufacturers' data manufacturers' safety and data, because they are unaware of the data that are kept and used by these businesses, government agencies, and other organizations. Another person isn't sure if he would ever buy them again. It is evident from the response to this query that most will repurchase these devices.

6. Discussions and Findings

The study's thorough analysis revealed that almost all participants have multiple IoT-based smart devices, meaning that IoT adoption is nearly 100%. In general, participants have strong general knowledge, understanding, and technical awareness. Young people in the 20–35 age range are more passionate, technologically savvy, and intrigued about new devices. People between the ages of 50 and 60, as is to be expected, have minimal technical understanding and only wish to use technology when absolutely necessary to improve their daily life at home and make them feel more secure. According to experimental investigation, the advantages of IoT devices include improved productivity, cost savings, the use of visual aids, and increased comfort in daily life.

Despite the lack of clarity surrounding the security and privacy concerns related to smart gadgets, poor neglect has emerged as one of the main problems. What information is gathered, how it is obtained, and to what extent is unclear to the participants. They are unaware of the purchase agreement's conditions and privacy policies. Participants felt uneasy disclosing their personal information to outside businesses. 85 percent of software and 58 percent of IoT-based smart devices reveal personal data to outside parties. The most frequent sorts of data supplied by these external devices and businesses are local data and IP addresses. Previous studies have revealed that while analyzing smart home gadgets like TVs, virtual assistants, smart speakers, door knobs, and electronics, they communicated user information to third-party businesses like Netflix, Spotify, Microsoft, etc.

According to the empirical results and their analysis, the following patterns or similarities can be seen in the data that has been gathered:

6.1. Learn about the IoT and smart homes

The initial study showed that the targeted respondents were knowledgeable about IoT and the ideas of smart homes.

6.1.1. Use of smart devices and technology

Participants' knowledge of technology and their use of smart devices in their homes appear to be another recurring feature. In their houses, all 10 individuals employ both conventional and cutting-edge technology, including electronics, smartphones, and watches.

6.1.2. IoT gadgets like better life quality

Another common belief is that technology and smart devices help make daily activities and life more comfortable and stress-free. Participants of all ages stated that they purchased these tools and gadgets in order to complete various chores more quickly, cheaply, and laboriously. These include booking a trip, manipulating smart locks, organizing an outing, adjusting lighting and heating from a mobile device, playing beloved music, and reserving particular favorites for visible aid so they may pick you up when they get home from work or on vacation.

6.1.3. Normal safety tightness

Surprisingly, awareness and rigor in fundamental security procedures are another point of commonality. Participants routinely change their passwords. We adhered to the standard password standards of using medium-to-strong passwords. Even participants in their middle years and elder years very infrequently reviewed their passwords. To save their credentials in a safe and secure location, participants used "password vaults," and they also used passwords to access their rooms.

6.1.4. False security and a lack of awareness of confidentiality

Although consumers are checking their router passwords, it is discovered that they are less inclined to change the passwords for their smart home gadgets. Not knowing the true harm posed by information or data leaks, exploitation, and misuse is concerning. All participants are found to have a reasonable level of knowledge and awareness when it comes to understanding how risky they are, the types of risks involved, and the potential outcomes.

6.1.5. Third-party participation

Another crucial issue is the collecting of data and its unauthorized usage or even sale without the participants' knowledge. The makers of devices and gadgets gather consumer information. Many times, participants are unaware of the extent to which local governments, businesses, and multinational organizations had access to their personal data. It has been reported that this frequently occurs without the participants' consent.

Certification, authorization, trust, secrecy, third-party data, and the identified access control features are all intimately connected to these categories and the findings mentioned above. To cope with it, there are numerous options. For IoT devices, it is crucial to employ digital signatures and certificates. It is crucial to keep in mind that the majority of certification and signature-based verification procedures rely on a dependable third party or certification body to confirm the person's identification. Strong passwords are also crucial in this situation. It is challenging to directly apply complex IoT-based solutions since the general public is not particularly tech-savvy or because it depends on the age group using IoT devices. This shows that in order to manage login, access to all information, and task management on smart home devices, people need to have some basic to moderate technical skills. Academics in education believe that power-based instruction should be used to teach IoT users. Other significant difficulties are the data's integrity and confidentiality. They didn't know which device was being used or how much data it was collecting. People should carefully read the product description of their IoT product to gain a basic understanding of how the device functions and to use their home network and other resources. People should take into account the kind of encryption that their device offers.

The use of encryption and cryptography techniques is the primary method for ensuring confidentiality and integrity on smart home devices. Symmetric and asymmetric data encryption are two widely used techniques. Both are applicable to IoT devices. Although each scheme offers a unique mix of benefits and drawbacks, it is clear from the actual findings that individuals are only interested in what would make it comfortable and easy to use, and have little interest in anything else. Because young and middle-aged people had a lot of technical know-how, they wanted and needed to look at gadgets that provide access to devices using digital signatures and hash functions to maintain the integrity of their smartwatches, smart music systems, and smart, intelligent virtual assistants. Heating and lighting systems are the main components of the proof data. Furthermore, the expensive cost of procurement and uncertainty about future device security, particularly in light of the rapid advancement of technology, seem to be further obstacles for its few.

6.2. IoT and its associated risks, impacts, and user perceptions

Machine learning (ML) algorithms have become powerful tools for improving the security of IoT devices. An important use of machine learning (ML) in IoT security is the analysis of network traffic patterns to spot possible cyberattacks or unusual behavior in devices. Conventional security measures, like intrusion detection systems (IDS) and firewalls, frequently find it difficult to keep up with the constantly changing landscape of cyberthreats. ML-based methods provide a flexible and dynamic way to deal with this problem.

IoT devices can continuously monitor and analyze network traffic coming into and going out of the device by utilizing ML models. These models can identify departures from expected behavior that might point to a security breach because they were trained on sizable datasets that contain typical network behavior patterns. Unusual communication patterns with unknown or suspicious IP addresses or anomalous spikes in network traffic volume, for instance, may indicate the possibility of a cyberattack, such as a distributed denial-of-service (DDoS) attack or an attempt at unauthorized access.

Moreover, machine learning algorithms have the ability to identify patterns linked to particular categories of cyberthreats, like malware infestations or attempts at data exfiltration. ML models are able to precisely classify and prioritize security alerts by establishing correlations between different network features and contextual information. This allows for prompt mitigation and response actions. Furthermore, these models are capable of changing and growing as new threats arise, providing strong defense against evolving security threats.

The scalability and real-time functionality of machine learning (ML)-based security solutions for IoT devices is a major benefit. Traditional manual methods for security monitoring and incident response become unworkable as the volume and complexity of

IoT deployments keep growing. Massive amounts of network traffic data can be automatically analyzed in real time by ML algorithms, which makes it possible to quickly identify and mitigate security risks throughout extensive IoT ecosystems.

Nevertheless, there are drawbacks to implementing ML-based security solutions in IoT environments. These include the requirement for ample computational resources and access to high-quality training data. In order to reduce the risks connected with adversarial attacks or data breaches, it is also crucial to guarantee the integrity and privacy of sensitive data that is gathered for the purpose of training machine learning models. In spite of these obstacles, the incorporation of machine learning algorithms into IoT security frameworks has great potential to improve the security posture and resilience of IoT devices against constantly changing cyberattacks.

6.3. Natural Language Processing (NLP) in relation to privacy regulations

IoT device privacy policies using natural language processing (NLP) techniques are used to glean important details about data collection, storage, and sharing procedures. This can assist users in making more informed decisions by helping them comprehend the privacy implications of using these devices.

6.3.1. AI-powered maintaining privacy methods

AI-driven methods can be used in IoT systems to improve privacy protection while preserving the ability to do meaningful data analysis, such as federated learning or differential privacy. This could allay worries about how personal information gathered by IoT devices might be misused.

6.3.2. AI-based user authentication

AI algorithms, like facial recognition or behavioral biometrics, can be used in IoT devices to authenticate users. These technologies can improve device security by offering strong authentication procedures that are challenging for intruders to get around.

6.3.3. Personalized security recommendations driven by AI

AI systems examine users' device usage habits and offer tailored security advice. These systems might, for instance, recommend firmware updates or configuration adjustments in response to particular security flaws linked to the user's IoT devices.

6.3.4. AI-driven education and awareness

When configuring and utilizing IoT devices, users can receive real-time advice on security and privacy best practices from chatbots or virtual assistants powered by AI. These AI programs can provide tutorials, respond to user inquiries, and alert users to possible dangers.

Therefore, AI-powered predictive maintenance systems can increase the security and dependability of IoT devices by foreseeing possible security flaws or hardware malfunctions before they become serious problems. By being proactive, you can reduce downtime and stop security breaches.

7. Conclusion

The goal of the study is to present a summary of the most significant elements of the IoT, with a focus on the security, integrity, and privacy issues that the device poses as well as public awareness of these dangers. What security, privacy, and trust challenges are linked with IoT devices? How well-versed and concerned are individuals with security, privacy, and security in relation to IoT devices? What aspects should consumers take into account when purchasing and utilizing IoT devices? The following is done in response to these queries: After a thorough analysis of the literature, a list of security and privacy threats is created. In relation to the study's evidence, these dangers are addressed and examined. Strong conclusions are made, and study of the fundamental theory assists in familiarizing people with common sense in the context of security and privacy concerns relating to IoT devices. The results demonstrated how much people know about the dangers of IoT devices in relation to their technological interest and age. In a similar vein, compared to adults, young people appeared to be quicker, more alert, and more motivated to learn about security and privacy as well as how to safeguard their equipment. The majority of individuals are aware of the dangers that IoT devices pose, but they haven't taken any action to actively secure them. Lack of understanding about how to protect electronics and equipment is the root of the problem. People might not be able to verify the validity, authenticity, and dependability of their electronics' security features when buying and using them. Future research in privacy and security should focus on "why current solutions fail to protect security opportunities and what best practices should be followed to avoid such situations in the future." In order to tackle these security and privacy concerns, the researcher should also concentrate on collaborative team efforts. A crucial study question is how the government and IoT equipment makers view the problem of privacy and security in the context of smart home features.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Sangeetha S. K. B.: Conceptualization, Methodology, Software, Formal analysis, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Project administration. **Sandeep Kumar Mathivanan:** Methodology, Validation, Investigation, Supervision. **Saurav Mallik:** Validation, Investigation, Supervision. **Hong Qin:** Validation, Investigation, Supervision.

References

[1] Waheed, A., Umar, A. I., Zareei, M., Din, N., Amin, N. U., Iqbal, J., . . . , & Mohamed, E. M. (2020). Cryptanalysis and improvement of a proxy signcryption scheme in the standard computational model. *IEEE Access*, *8*, 131188–131201. https://doi.org/10.1109/ACCESS.2020.3009351

[2] Radanliev, P., De Roure, D. C., Nurse, J. R., Mantilla Montalvo, R., Cannady, S., Santos, O., . . . , & Maple, C. (2020). Future developments in standardisation of cyber risk

in the Internet of Things. *SN Applied Sciences*, *2*, 1–16. https://doi.org/10.1007/s42452-019-1931-0

[3] Sangeetha, S. K. B., Dhaya, R., & Kanthavel, R. (2019). Improving performance of cooperative communication in heterogeneous manet environment. *Cluster Computing*, *22*, 12389–12395. https://doi.org/10.1007/s10586-017-1637-2

[4] Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of Things: A systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting and Social Change*, *136*, 285–297. https://doi.org/10.1016/j.techfore.2018.01.022

[5] Hundera, N. W., Mei, Q., Xiong, H., & Geressu, D. M. (2020). A secure and efficient identity-based proxy signcryption in cloud data sharing. *KSII Transactions on Internet and Information Systems (TIIS)*, *14*(1), 455–472. https://doi.org/10.3837/tiis.2020.01.025

[6] Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, *21*(5), 1809. https://doi.org/10.3390/s21051809

[7] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, *20*, 2481–2501. https://doi.org/10.1007/s11276-014-0761-7

[8] Khan, M. A., Shah, H., Rehman, S. U., Kumar, N., Ghazali, R., Shehzad, D., & Ullah, I. (2021). Securing internet of drones with identity-based proxy signcryption. *IEEE Access*, *9*, 89133–89142. https://doi.org/10.1109/ACCESS.2021.3089009

[9] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*, 423–441. https://doi.org/10.1007/s11235-017-0345-9

[10] Oracevic, A., Dilek, S., & Ozdemir, S. (2017). Security in Internet of Things: A survey. In *2017 International Symposium on Networks, Computers and Communication*, 1–6. https://doi.org/IEEE.10.1109/ISNCC.2017.8072001

[11] Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188–2204. https://doi.org/10.1109/JIOT.2018.2882794

[12] Guo, H., & Deng, L. (2020). An identity based proxy signcryption scheme without pairings. *International Journal of Network Security*, *22*(4), 561–568.

[13] Mącik, R. (2017). The adoption of the internet of things by young consumers – An empirical investigation. *Economic and Environmental Studies*, *17*(2(42)), 363–388. https://doi.org/10.25167/ees.2017.42.13%0A

[14] Jurcut, A., Niculcea, T., Ranaweera, P., & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. *SN Computer Science*, *1*, 1–19. https://doi.org/10.1007/s42979-020-00201-3

[15] Sangeetha, S. K. B. (2019). An empirical investigation of securing internet of things data in wireless sensor network. *Journal of Asian Scientific Research*, *9*(8), 95–99. https://doi.org/10.18488/journal.2.2019.98.95.99

[16] Weyrich, M., & Ebert, C. (2015). Reference architectures for the internet of things. *IEEE Software*, *33*(1), 112–116. https://doi.org/10.1109/MS.2016.20

[17] Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., & Alazab, M. (2020). Blockchain-envisioned secure data delivery and collection scheme for 5g-based IoT-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology*, *69*(8), 9097–9111. https://doi.org/10.1109/TVT.2020.3000576

[18] Khan, M. A., Ullah, I., Nisar, S., Noor, F., Qureshi, I. M., Khanzada, F. U., & Amin, N. U. (2020). An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network. *IEEE Access*, *8*, 36807–36828. https://doi.org/10.1109/ACCESS.2020.2974381

[19] Khan, M. A., Ullah, I., Kumar, N., Oubbati, O. S., Qureshi, I. M., Noor, F., & Khanzada, F. U. (2021). An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks. *IEEE Transactions on Vehicular Technology*, *70*(5), 4839–4851. https://doi.org/10.1109/TVT.2021.3055895

[20] Hsu, W. L., Qiao, M., Xu, H., Zhang, C., Liu, H. L., & Shiau, Y. C. (2021). Smart city governance evaluation in the era of internet of things: An empirical analysis of Jiangsu, China. *Sustainability*, *13*(24), 13606. https://doi.org/10.3390/su132413606

[21] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, *9*, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408

[22] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*, 261–274. https://doi.org/10.1007/s10796-014-9489-2

[23] Bali, S., Bali, V., Gaur, D., Rani, S., Kumar, R., Chadha, P., . . . , & Vatin, N. I. (2023). A framework to assess the smartphone buying behaviour using DEMATEL method in the Indian context. *Ain Shams Engineering Journal*, *102129*. https://doi.org/10.1016/j.asej.2023.102129

[24] Srividya, N., Atiq, R., & Volety, N. S. (2024). Qualitative research on responsible consumption concerning apparel. *Cleaner and Responsible Consumption*, *12*, 100178. https://doi.org/10.1016/j.clrc.2024.100178

[25] Reshi, I. A., Dar, S. A., & Ansar, S. S. (2023). An empirical study on the factors affecting consumer behaviour in the fast-food industry. *Journal of Accounting Research, Utility Finance and Digital Assets*, *1*(4), 376–381. https://doi.org/10.54443/jaruda.v1i4.58

[26] Rathi, R., Jain, S., & Garg, R. (2023). Exploring young consumer's adoption of secondhand luxury: Insights from a qualitative study. *Journal of Fashion Marketing and Management: An International Journal*, *28*(1), 117–138. https://doi.org/10.1108/JFMM-11-2022-0236

[27] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41–70. https://doi.org/10.1016/j.iot.2018.11.003

[28] Shaik, M. (2023). Impact of artificial intelligence on marketing. *East Asian Journal of Multidisciplinary Research*, *2*(3), 993–1004. https://doi.org/10.55927/eajmr.v2i3.3112

[29] Kumar, S. (2023). An exploratory study of millennial consumer behavior antecedents using influencer marketing. *Academy of Marketing Studies Journal*, *27*, 1–16.

[30] Vidani, J., Meghrajani, D. I., & Das, S. (2023). Unleashing the power of influencer marketing: A study on millennial consumer behaviour and its key antecedents. *Journal of Education: Rabindra Bharati University*, *25*(6), 99–117.

[31] Grover, Y. (2023). Digital transformation in marketing: Prospects and challenges. *IUJ Journal of Management*, *11*(1), 218–228.

[32] Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, 97–108. https://doi.org/10.1016/j.eswa.2019.05.014

[33] Yesmin, T., Carter, M. W., & Gladman, A. S. (2022). Internet of things in healthcare for patient safety: An empirical study.

BMC Health Services Research, *22*(1), 278. https://doi.org/10.1186/s12913-022-07620-3

[34] Haddud, A., DeSouza, A., Khare, A., & Lee, H. (2017). Examining potential benefits and challenges associated with the Internet of Things integration in supply chains. *Journal of Manufacturing Technology Management*, *28*(8), 1055–1085. https://doi.org/10.1108/JMTM-05-2017-0094

[35] Chatterjee, S. (2020). Internet of Things and social platforms: An empirical analysis from Indian consumer behavioural perspective. *Behaviour & Information Technology*, *39*(2), 133–149. https://doi.org/10.1109/ACCESS.2021.3073408

[36] Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 IEEE World Congress on Services*, 21–28. https://doi.org/10.1109/SERVICES.2015.12

[37] Kanthavel, R., Sangeetha, S. K. B., & Keerthana, K. P. (2021). Design of smart public transport assist system for metropolitan city Chennai. *International Journal of Intelligent Networks*, *2*, 57–63. https://doi.org/10.1016/j.ijin.2021.06.004

[38] Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, 68–90. https://doi.org/10.1016/j.adhoc.2014.12.006

[39] Saleh, M., Jhanjhi, N. Z., Abdullah, A., & Saher, R. (2022). Proposing encryption selection model for IoT devices based on IoT device design. In *2022 24th International Conference on Advanced Communication Technology,* 210–219. https://doi.org/10.23919/ICACT53585.2022.9728914

[40] Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: Challenges and key issues. *Security and Communication Networks*, *2021*(1), 5533843. https://doi.org/10.1155/2021/5533843

How to Cite: S. K. B., Sangeetha, Mathivanan, S. K., Mallik, S., & Qin, H. (2025). Ground Theory Based Empirical Analysis of Security Issues and Challenges Associated with Internet of Things. *Artificial Intelligence and Applications*. https://doi.org/10.47852/bonviewAIA52022523