

A Web-based User-Interface for Internet of Things Device Management

by

Leena Mansour Alghamdi

A thesis

submitted to the Department of Computer Engineering and Sciences of

Florida Institute of Technology

in partial fulfillment of the requirements

for the degree of

Master of Science

in

Information Assurance and Cybersecurity

Melbourne, Florida

July 2020

© Copyright 2020 Leena Mansour Alghamdi

All Right Reserved

The author grants permission to make single copies.

We the undersigned committee hereby approve the attached thesis, “Title: A Web-based User-Interface for Internet of Things Device Management” by Leena Mansour Alghamdi

Heather Crawford, Ph.D.
Assistant Professor
Department of Computer Engineering and Sciences
Committee Chair

Meredith Carroll, Ph.D.
Associate Professor
School of Aeronautics
Outside Committee Member

Michael King, Ph.D.
Associate Professor
Department of Computer Engineering and Sciences
Committee Member

Philip Bernhard, Ph.D.
Associate Professor and Department Head
Department of Computer Engineering and Sciences

Abstract

Title: A Web-based User-Interface for Internet of Things Device Management

Author: Leena Mansour Alghamdi

Advisor: Heather Crawford, Ph.D.

With the growing advances in the Internet of Things (IoT) technology, which combines various devices with distinct functions, capabilities, and communication protocols, it is essential to provide a platform that enables IoT users to interact with their IoT devices directly and be able to manage them effortlessly via that platform from various locations at any time in order to protect their privacy when using IoT devices. In this study, we are aiming to provide a web-based user interface that can address that challenges and provide real-time data control; hence, we have created a user interface prototype, which can demonstrate the concept of IoT manager websites and provide a proof of concept implementation. As the proposed platform is intended to contribute to improving users' perception of the IoT devices. Furthermore, the experimental and survey methods are used in this study to assess the participants' perception of using one platform that combines all of their IoT devices and enables

them to protect their privacy by managing these devices based on their preferences via the platform. The findings showed the need for creating a platform where users can control various IoT devices remotely. It also indicated that the website prototype is a user-friendly platform, and it could be used easily without any technical experience. Users were able to access information about the connected IoT device as well as control it.

Table of Contents

Abstract	iii
List of Figures	x
List of Tables	xii
Abbreviations	xiii
Acknowledgement	xiv
1 Introduction	1
1.1 Research Problem	2
1.2 Our Proposed Solution: A Web- based User-Interface for Internet of Things Device Management	4
1.2.1 Research Question	4
1.2.2 Research Hypotheses	5
1.3 Thesis Structure	6
2 Literature	7
2.1 Introduction to IoT	7
2.1.1 Definition of "Things".	10
2.1.2 Goals of IoT.	11

2.1.3 Components of IoT	12
2.1.4 Architecture of IoT.	15
2.1.5 Applications of IoT	18
2.1.6 Particular Qualities of IoT	20
2.1.7 Technologies of IoT.	22
2.2 Security Threats in IoT.	25
2.2.1 Application Layer Threats.	26
2.2.2 Perception Layer Threats	27
2.2.3 Network Layer Threats	28
2.2.4 Physical Layer Threats	29
2.3 Ensuring Security in IoT	31
2.3.1 Application Layer Security.	31
2.3.2 Perception Layer Security	32
2.3.3 Network Layer Security	33
2.3.4 Physical Layer Security	34
2.4 Privacy Issues in IoT	35
2.5 Privacy Protection	39
2.5.1 Authentication and Authorization	41
2.5.2 Edge Computing and Plug-in Architecture	43
2.5.3 Data Anonymization	44
2.5.4 Digital Forgetting and Data Summarization	44

2.6 Privacy Protection in Layers of IoT	46
2.6.1 In Application Layer	46
2.6.2 In Network Layer	48
2.6.3 In Perception Layer	50
2.7 Privacy-by-Design Principle	52
2.8 Summary	53

3 Design and Methodology 55

3.1 Introduction	55
3.2 Related Work	56
3.3 The Proposed Platform	58
3.3.1 Detailed Description.	61
3.4 The Proposed Prototype.	65
3.4.1 The Prototype Website Structure	65
3.4.1.1 Home Page	66
3.4.1.2 Categories Page	67
3.4.1.3 Account Page.	68
3.4.2 The Prototype of IoT Device	69
3.4.3 The Website Weaknesses	70
3.4.4 Expected Feedback	71
3.5 Summary	71

4 User Study and Findings	72
4.1 General Purpose	72
4.1.1 Specific Aims	73
4.1.2 Research Questions	73
4.1.3 Hypothesis	74
4.2 Study Design Description: Instruments and Methods	75
4.3 Participants Characteristics	76
4.3.1 Sampling Technique	77
4.4 Data Acquisition	77
4.4.1 Structure of the Survey	79
4.5 Data Analyses and Results.	80
4.5.1 Demographic Information.	80
4.5.2 Primary Analysis	83
4.5.2.1 Descriptive Statistics	83
4.5.2.2 Inferential Statistics	88
4.5.3 Supplementary Analysis	91
4.5.3.1 Participants' Understanding of the Website (User-Interface Web App)	91
4.5.3.2 IoT Devices' Usage	93
4.5.3.3 Participants' Privacy Attitudes	95

4.5.3.4 Participants' Willingness to take Actions in order to Protect their Personal Information that is Captured by IoTDevices.	97
4.6 Discussion	101
4.7 Study Limitations	109
4.8 Summary	110
5 Conclusion and Future Work	112
5.1 Research Questions and Research Hypotheses.	113
5.2 Future Work	116
References	117
A - IRB Approval	136
B - A Web-based User-Interface for Internet of Things Devices' Management Questionnaire	137

List of Figures

Figure 1 — Layers of IoT	17
Figure 2 — Data Flow Diagram of the Website	64
Figure 3 — The Web App Structure	66
Figure 4 — Home Page	67
Figure 5 — Categories Page	68
Figure 6 — Account Page	69
Figure 7 — Data Visualization from BMP180 Sensor	70
Figure 8 — Number of Hours Using IoT Devices	82
Figure 9 — Privacy and Convenience Importance	84
Figure 10 — Importance of Actions to Protect Personal Information	86
Figure 11 — The Effect of the Amount of Use of IoT Devices by Users on the Importance of Some Actions to Protect Personal Information	87
Figure 12 — Participants' Satisfaction of the Website	88
Figure 13 — How Many IoT Devices are Currently Connected to the Website	91
Figure 14 — How Many Temperature Readings are Currently Listed for the BMP180 Temperature and Pressure Sensor?	92
Figure 15 — What was the Temperature Reading at 07:28:44 on 10/24/2019?	92
Figure 16 — Data Captured by Specific IoT Devices	95

Figure 17 — Statement Rank	97
Figure 18 — Participants' Responses (Privacy Concerns)	98
Figure 19 — Participants' Responses (Using Website for IoT Devices Management)	99
Figure 20 — Participants' Responses (Use One Platform for all IoT Devices)	100
Figure 21 — Hypothetical Scenario Responses	101

List of Tables

Table 1	Participants' Demographic Information	81
Table 2	Categorizing the Participants Based on their Use of IoT Devices	85
Table 3	P-value for Each Action	90
Table 4	IoT Devices' Usage	94
Table 5	Privacy in Daily Life	96

Abbreviations

IoT	Internet of Things
UI	User Interface
IP	Internet Protocol
RFID	Radio Frequency Identification
BLE	Bluetooth Low Energy
NFC	Near Field Communication
U2IoT	Unit and Ubiquitous IoT
WSN	Wireless Sensor Network
Wi-Fi	Wireless Fidelity
API	Application Programming Interface

Acknowledgments

First and foremost, I am grateful to the God, the Almighty, for the good health and wellbeing that were necessary to complete this thesis successfully. The path toward this thesis has been circuitous. Its completion is thanks in large part to the special people who challenged, supported, and stuck with me along the way.

I would like to express my sincere thanks to my advisor, Dr. Heather Crawford, and my committee members, Dr. Meredith Carroll and Dr. Michael King, for their great help and giving thoughtful feedback.

I am grateful to all the participants who participated in the survey that was conducted in this work. I am also thankful to the government of Saudi Arabia represented by Albaha University for their financial support.

Nobody has been more important to me in the pursuit of this work than the members of my family. I owe more than thanks to my parents, sister, and brothers for their love, prayers, caring, and encouragement throughout my life. I am extending my heartfelt thanks to my mother-in-law for her valuable prayers and caring. Most importantly, I must express my profound gratitude to my loving and supportive husband, Faisal, who has stood by me and who has been patient while working on this thesis. He provided me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis, and to my wonderful daughter, Talia, who provides unending inspiration. She

gave me unlimited happiness and pleasure. This accomplishment would not have been possible without them.

Chapter 1

Introduction

The phenomenal development in the Internet of Things (IoT), has led to a revolution in the technology field. IoT can be defined as a system that combines different devices, actuators, sensors, communications protocols, and applications that can independently exchange data and commands through networks to provide intelligent services. In addition, it embraces various applications, services, and communication technologies, allowing for ubiquitous data collection and tracking to provide smart services that can improve people's lives. According to Gartner's forecast [1], 20.4 billion connected objects will be in use worldwide by 2020. Whereas these massive numbers of connected devices are invading our surroundings and capturing our sensitive information without our knowledge nor our permission.

1.1 Research Problem

Through the tremendous development in smart devices, it has been observed that many devices have no way for those interactions and communications with users such as screens, or user interface. IoT users need a way to interact with their devices to view the data captured by IoT devices. As a result, there is a need to create a user interface (UI) that includes screen, buttons, and forms that enables users and computer system including IoT systems to interact and communicate with each other.

Furthermore, a critical privacy issue that associated with information technology has appeared since the widespread of systems that capture users' data while they are using Internet-connected devices or even when they are in a public place which is full of sensors which can capture the people's data without their knowledge or consent. According to [2], the problem is that third parties have not given permission to be part of the data collection in a public area. For example, bystanders were found in the captured photos by strangers. The importance of this issue has increased because of the spread of mobile and Internet-connected devices everywhere. Actually, the potential privacy invasion can be in places where people do not expect to be under surveillance. At the same time, if they knew that they were being watched, it would not be considered a privacy breach, this is because people are likely to behave differently in public areas if they know they are going to be being

filmed the whole time. Not to mention their homes, where people want to experience their full comfort and freedom without any monitoring of their actions or capturing their sensitive information. Therefore, people may have concerns about their data privacy, as they may want to know who is observing their information. Hence, they do not feel comfortable using or selling their sensitive data to a third party [3]. In fact, people care about the techniques used for sharing their confidential data more than just the shared data itself. Where most of them think the violation of privacy happen when their data has been shared for inappropriate purposes. Besides, due to the proliferation of IoT devices and the diversity of data collection and use by these devices, people's perception of this innovative technology may change over time. In addition, because of the collection of data has become more accessible, and it can be achieved without people's awareness so that many of the IoT services may be avoided by many people due to the invisible collection and processing of data. Therefore, there is an urgent need to understand people's different perspectives about the IoT devices that associated with privacy issues and finding convenient and straightforward solutions to preserve their privacy by fulfilling their various privacy preferences in IoT devices, which in turn contribute to changing people's perceptions.

1.2 Our proposed Solution: A Web-based User-Interface for Internet of Things Devices' Management

To address these issues related to the privacy, user-interaction, controlling in IoT devices, we propose a system (Web-based User-Interface) for IoT devices that allows IoT users to interact with their devices and also connect and manage the IoT devices through that interface. Thus, it is intended for the improvement of IoT users' privacy perceptions, in which IoT devices collect and transparently use users' information to ensure that users' privacy requirements are met. The implemented work in this study is a prototype that will contribute to delivering the concept of the web-based user interface for IoT users to connect their IoT devices to the website and then manage those connected devices through that website.

1.2.1 Research Questions

The following research questions define the research in this thesis:

Q 1- When using smart devices, is privacy or convenience more important for users?

Q 2- Does the amount of IoT device use by users have an effect on the importance of the following actions to them: “allowing users to control what information is

collected about them, informing users when their information is collected, and requesting users' permission to collect their information”, to protect their personal information that is captured by IoT devices?

Q 3- To what extent does offering an independent web interface, which does not require a specific operating system or separate software development for IoT devices management, gain users' satisfaction?

1.2.2 Research Hypotheses

The following hypotheses are drawn from the research question:

H 1- When users use smart devices, privacy is more important to them than convenience.

H 2- The users' usage amount of IoT devices does not affect the importance of the following actions to them: allowing users to control what information is collected about them, informing them when their personal information is collected, and requesting their permission to collect their information before it is collected, in terms of protecting their information that is captured by IoT devices.

H 3- When the participants experience the web-user interface (The prototype of our website), they will be satisfied with the website organization, ease of the website navigation, and the user interface.

1.3 Thesis Structure

This thesis is organized as follows: Chapter 2 reviews the literature of IoT, its definition, history, architecture, and its applications, then outlines the privacy issues of IoT and the recent research contributions to overcome these issues. Chapter 3 describes the process of designing and implementing our proposed website. Chapter 4 describes the user study, highlights the findings, and provides an outlook of the future work that needs to be conducted in this area. Finally, Chapter 5 concludes the research.

Chapter 2

Literature Review

This chapter presents an overview of IoT, its definition, its history, and its applications, also highlights the architecture design of IoT that consists of different layers. This chapter addresses the security threats and privacy issues in IoT that relied on various dimensions, and the final part in this chapter discusses some techniques to ensure security and protect privacy in IoT, with a brief description of the Privacy-by-Design Principle.

2.1 Introduction to IoT

The term of the Internet of Things has cut across many areas of today's human lifestyle, which can be defined as a system that combines different devices, actuators, sensors, communications protocols, and applications that can independently exchange data and commands through networks to provide intelligent services. This recent technology has expanded and developed rapidly in recent years. In 1999 in the RFID journal was the first use of the term of the Internet of Things by the inventor of IoT Kevin Ashton from the Massachusetts Institute of Technology's (MIT), who was the co-founder and executive director of the Auto-ID Center. Ashton said that “I

could be wrong, but I am fairly sure the phrase 'Internet of Things' started life as the title of a presentation I made at Procter & Gamble in 1999.” [4]. Since the advent of the Internet of Things, it has been developed in stages. In 2005, the UN's International Telecommunications Union (ITU) published its first report on the Internet of Things. They expanded its meaning, addressing that the communication of machines with each other or with people is extended to objects, including daily common objects and sensors in various elements [5]. Therefore, according to the ITU, the Internet of Things is a virtual world representing the real world, in which things can communicate with each other and with people as well, as long as everything in the real world has its own identity in the virtual world [5]. In 2008, the IPSO Alliance was launched by a group of more than 50 companies to promote and support the use of Internet Protocol (IP) of "smart objects" and to enable the Internet of Things. Furthermore, the Internet of Things registered as one of the 6 "Disruptive Civil Technologies" with potential impacts on US interests out to 2025 by the U.S. National Intelligence Council [6]. Then, in the Cluster of European Research Projects on the Internet of Things (CERP-IoT), the European Commission defined the IoT as “a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network” [7]. Huang and Li [8] discussed the semantic meaning of the term Internet of Things, and they

defined the IoT as sharing information globally among interconnected objects. Coetzee and Eksteen [9] portray the IoT as part of the future Internet. The expansion of the Internet causes the Internet of Things developed by enabling the physical objects to provide intelligent services, where every object has a unique identifier and can access to the network, with the ability to determine its position and status. According to Miorandi et al. [10], the Internet of Things is an extension of the traditional Internet, where the Internet used by the IoT to enable communication, computing, and coordination between the machines and smart objects. In the field of ubiquitous computing, Gubbi et al. [11] defined the IoT as the "interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications." [11]. However, though the IoT definitions are seemingly diverging, they are usually presented around five elements: networking, services, communications, data, and things. The networking aspect was the center of most definitions previously, while the most recent intent to be more comprehensive [12]. From the previous perspectives, the Internet of Things can be defined as a combination of the connected wireless devices, networks, sensors, processors, and smart applications that have combined to provide an intelligent service. Besides, connecting the various devices and connecting them to the Internet, enabling users to benefit from each device. The necessity of connecting the physical devices to the Internet is the inability of a human to control all devices simultaneously.

Additionally, IoT's devices provide increased quality of services in any organization and improve productivity by offering in-time training for the employees [13] and increasing the possibilities of remote working, and this can significantly increase overall productivity while reducing power consumption. In 2015, Gupta et al. [14] proposed a power-efficient Ethernet-based automatic control system for controlling the electrical devices by the IoT devices of the institutional buildings. The model is deployed in the classroom to control its lights and save energy. The proposed system has high performance in minimizing computation power. Therefore, the IoT devices and applications can communicate with each other to make decisions on behalf of a human being. Practically, the IoT can capture users' data via sensors, send, receive, and share in some cases, the captured information from the users. No organization in the world controls and owns the IoT completely; therefore, there are no accurate and consistent definitions of the IoT. However, various entities and many organizations intended to clarify the term of the Internet of Things and define it accurately and clearly.

2.1.1 Definition of “Things”

The definition of "Things" has been discussed for more understanding of IoT capabilities, which is an essential component of the IoT. Coetzee and Eksteen [9] defined things as a vast and include a set of different physical objects, includes

personal elements such as smartphones, and tablets and other elements in the surrounding environment that would be available in home, vehicle, and workplace, as well as objects fitted with RFID tag that connected to the devices. Furthermore, things considered objects. Elkhodr et al. [15] state that the IoT object is referring to any device, application, and physical element involved in an interaction and connection to the Internet with the ability to have access to digital information. The term "things" also refers to any object that connected to the Internet and has an IP address; it communicates via the network without direct human intervention.

2.1.2 Goals of IoT

The end goal of the Internet of Things is to provide a linkage between different systems; thus, they should interoperate and communicate automatically to provide an intelligent service to the IoT's users [16]. According to Ma [17], IoT has three essential goals, more extensive interconnection, more intensive information perception, and more comprehensive intelligent service. They are explained as follows [17]:

1- More Extensive Interconnection: the interconnection in the IoT devices expanded from ordinary objects to intelligent or non-intelligent elements. It has some features:

- A. Extensiveness in the number of devices. The connected devices will expand dramatically, containing sensors, actuators, and RFID devices.
- B. Extensiveness in the type of devices. Devices in a particular network may be provided by a direct electronic power or by batteries.
- C. Extensiveness in the connection mode. There are two ways of connection between devices which are by wire or wireless with a strong or weak state routing, and two types of communication that are a single hop or multiple hops.

2- More Intensive Information Perception: The IoT has developed a new paradigm of the collaboration of multi-sensors due to the uncertainties in capturing information from a single sensor.

3- More Comprehensive Intelligent Service: The comprehensive smart services can be provided by the IoT that allows the physical devices to participate directly in the services process without people intervention.

2.1.3 Components of IoT

Generally, according to Hsu [18], the whole picture of the IoT is consist of six main components that execute substantial procedures:

1. Sensors to capture data from the surrounding environment. These sensors include accelerometer sensors, proximity sensors, infra-Red (IR) sensors, temperature sensors, chemical sensors, magnetometers, altimeters, and other.
2. Processors that process the captured data. There are several options for the processors such as Media Tek MT3620, On Semi RSL10, ETA Compute Tensai, Microchip SAM R34/35, NCP i.MX-RT600, and Renesas Electronics RZ/A2M.
3. Different technologies to connect the data to the networks. These technologies are ranging from the bottom of the protocol stack to the top of the stack, which are LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC, and RFID.
4. IoT platforms and software that perform data analysis. The examples of the software that used to extract valuable and meaningful information from the captured data are best for smart home, Amazon for IoT SaaS (Software-as-a-Service), AeroScout for connected health, and many other platforms.
5. Smart applications that benefit from the information to improve efficiency and increase productivity. Including smart homes, smart cars, smart buildings, smart health, smart cities.
6. Intelligence services that are provided to the consumers are critical in order to achieve the purposes of the IoT. Services encompass building automation,

intelligent navigation, tracking system, vehicle management system, in addition to other services that help in enhance objects utilization.

The essential organization of an IoT system has shown in [19] as below:

- The *environment* is the physical system with which the IoT system interacts.
- A set of devices forms the network. A node contains sensors, actuators, processors, and memory, and a network interface is available for each node. A node may or may not run the Internet Protocol.
- Hubs provide the first-level connection between the nodes and the rest of the network.
- *Fog processors* perform operations on local sets of nodes and hubs. Fog devices also introduce system management issues, even with the lower compute power compared with cloud servers.
- *Cloud servers* provide computational services for the IoT system. Data and computational results are stored in *databases*. The cloud may provide a variety of services that mediate between nodes and users, such as storage capacity and processing capabilities.

2.1.4 Architectures of IoT

The mixed structure can be presented by the IoT that includes various subsystem architectures. IoT systems are formed by two management architectures: event-driven and time-based. In an event-driven architecture, the data is transmitted when sensors sense action in the outside surroundings. In the time-based architecture, based on a particular interval, data is continuously transmitted [20]. Although the key technologies and the underlying architecture of IoT are still open issues. However, numerous researchers have proposed various kinds of IoT architectures. One of the proposed architectures for future IoT incorporates social attributes is unit and ubiquitous IoT (U2IoT) [21].

The future IoT structure attended to link the physical world with the virtual world and the social world. Unite and ubiquitous IoT (U2IoT) used to combine the physical world with the cyber world. It includes diverse systems; U2IoTs include the industrial IoT, national IoT, and global IoT, which combine many Unit IoTs with ubiquitous characteristics. There are some significant features of the U2IoT model, which are virtual, physical, social co-existence, interconnection and interactivity, space-time consistency, and multi-identity status [22]. The components of a system are defined by IoT architecture, how to work collectively, and how data exchanged between them. Some different IoT architectures have been described below.

A. IoT Forum Architecture

IoT architecture is divided into three layers: Perception, Network, and Application layer. Each layer has its functionality. Perception layer to identify smart elements in the environment. The network layer is used for routing and processing of data. Application layer to provide services to users via different applications [23].

B. International Telecommunication Union (ITU) Architecture

IoT architecture is divided into five layers: The Sensing layer is for data gathering, the Access layer is for the interaction, the Network layer is for data transmission, the Middleware layer is for processing information, and the Application layer is for data representation.

For analyzing the different aspects of IoTs, such as security, privacy, and application, it is vital first to understand the architecture of IoTs. IoT consists of different layers interacting with all the time, each having a different set of instructions of the protocol. This difference in the structure of layers makes the challenges of security and privacy different for each layer, making it all the more important to understand the architecture of IoTs before understanding the security and privacy issues. The architecture of IoTs consisting of four layers, is briefly described below, adapted from the works [24], [25], [26]. The architecture of IoTs consists of four layers interacting with each other to pull out an IoT. These layers are as follows:

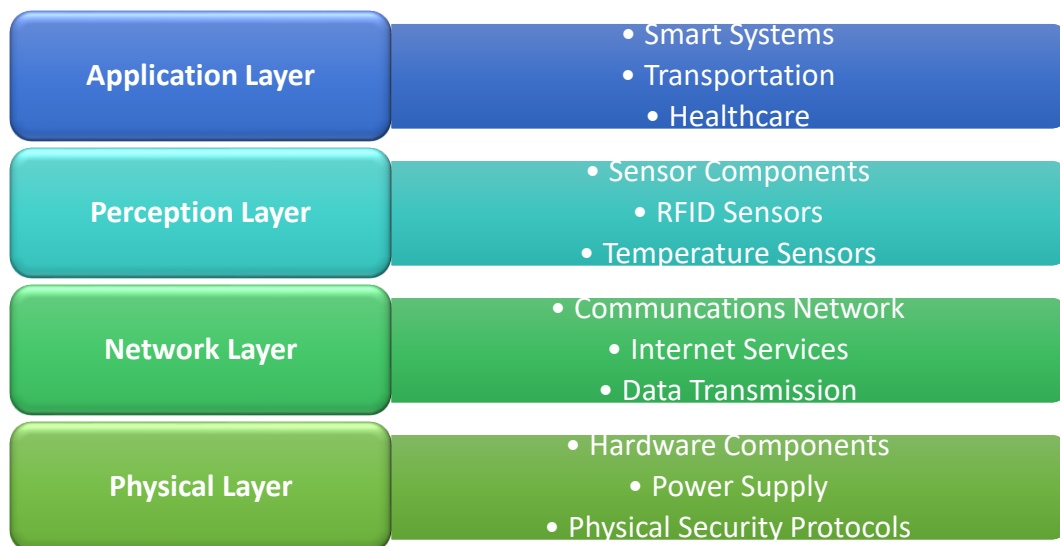


Figure 1- Layers of IoT

1. **Application Layer:** Application layer comprises of different applications that an IoT provides to the user. Typical applications include smart interaction systems, transportation, and healthcare.
2. **Perception Layer:** The perception layer is more of a sensory layer comprising of sensor nodes. It contains different sensors required for human interaction, such as temperature sensors, RFID sensors, geo-informatics sensors, and pressure sensors.
3. **Network Layer:** The network layer is responsible for developing two ways communications hence comprises of network communications software and physical and network components necessary for devices to communicate such as network nodes, servers, and topologies. As suggested by the name,

the network layer is responsible for transmitting and receiving data between devices and receivers.

4. **Physical Layer:** The physical layer is the outermost layer consisting of the necessary hardware required for human-computer interaction. These hardware components in the physical layer include smart appliances and power supplies.

2.1.5 Applications of IoT

Some of the essential example applications of IoT are briefly explained by Bandyopadhyay and Sen [27], in the following subsections:

1. **Aerospace and Aviation Industry:** Identify reliable products and elements by the Internet of Things that can help to improve the safety and security of products and services.
2. **Automotive Industry:** Advanced sensors and actuators will be available in cars, trains, buses, and bicycles to increase the quality of control. In addition to the use of smart things to monitor and report different parameters from pressure in tires to the proximity of other vehicles.
3. **Telecommunications Industry:** IoT will make the potential of the merging of varied telecommunications technologies and create new services. An illustrative example is the use of GSM, NFC (Near Field Communication),

low power Bluetooth, WLAN, multi-hop networks, GPS, and sensor networks, with SIM-card technology.

4. **Medical and Healthcare Industry:** There will be various IoT applications in the healthcare sector, with the potential of using the cell phone with RFID-sensor capabilities as a platform to monitor the medical parameters and drug delivery.
5. **Independent Living:** IoT services will have an essential impact on independent living by providing support for the aging population using wearable and ambient sensors to detect the activities of daily lives and monitor social interactions.
6. **Pharmaceutical Industry:** IoT paradigm will provide smart labels to drugs, tracking them through the supply chain, which allows to detect the counterfeit product and prevents fraud.
7. **Retail, Logistics, and Supply Chain Management:** Many advantages could be provided by IoT in retail and supply chain management (SCM) operations, such as RFID tags and smart shelves that track the present items in real-time.
8. **Manufacturing Industry:** Production processes and the entire lifecycle of products can be optimized and monitored by linking items with information technology, through embedded smart devices or the use of unique identifiers.

And some other varied applications:

Process Industry, Environment Industry, Transportation Industry, Agriculture, Media, Entertainment Industry, Insurance Industry, and Recycling [27].

Cooperation between platforms, applications, devices, and services enables improving citizens' well-being and quality of life. The enormous potentialities offered by the IoT make the development of a vast number of applications possible.

2.1.6 Particular Qualities of IoT

The IoT can include a vast number of integrated devices into local or global, physical, and wireless networks. The set of automated devices and sensors generates and transmits a vast amount of data in real-time, with adequate filtering and data processing.

- 1. Network Protocol:** Different network protocols such as Bluetooth, Wi-Fi, and ZigBee are the reason behind data transmission. Semantic and syntactic rules can determine the computer network actions.
- 2. Data Transmission:** Data transmission is one of the complicated processes in the IoT due to the consumption of many network resources. Information may vary based on the physical object type and transmission protocols. Thus, data transmission policy that is designed for network documents facilitates data analysis.

3. Heterogeneity: The most IoT key features is the IoT device heterogeneity. Based on a particular type of function procedure, the IoT architecture contains hybrid devices as well as it is divided into varied levels, where endpoint devices are located at the lowest vertical heterogeneity level, and the sophisticated routing and computing devices are moving to a higher level. Moreover, IoT heterogeneity contains various devices: personal tools, sensors, routers, databases, computing servers. IoT devices divided into three primary levels: endpoint devices that execute commands from outside entities or the central unit and generate data. IoT devices achieve the role of a mediator between endpoint devices and higher-level machines. The last level is computing machines that focus on data filtering and processing.

4. Scalability: Many factors affect the quantity of the components of the IoT structures in any system. However, third party technology can be used to tackle inconveniences, such as switches and routers, that allow for data exchange between an enormous number of IoT devices [20].

Eventually, the power of the IoT comes from its ability to perform a combination of the complicated processes without direct human interaction. Therefore, IoT intended to benefit from the considerable amount of users'

information by providing a common platform for the connected devices to take in their data. After that, perform the analysis on the integrated data from different resources to receive the required valuable information. Typically, sharing the results with other devices on the same network is needed for more advantageous features for the users.

2.1.7 Technologies of IoT

IoT includes multiple connected, intelligent devices with various embedded technologies, which are Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Cloud Computing, Wireless Fidelity (Wi-Fi), and ZigBee.

1. **Radio Frequency Identification (RFID):** The RFID system contains different components: tags transponders, tag readers, antenna, and an interface that used to identify an element wirelessly using radio waves. It includes reader and tags to identify and create signals which can be transmitted to the reader by RFID frequency and analyzed by the processors [28].
2. **Wireless Sensor Network (WSN):** It defined as self-configured and infrastructure-less wireless networks that have sensing capabilities to monitor physical and environmental conditions wirelessly, such as temperature, sound, vibration, and pressure. WSN consists of two main components which

are: sensor nodes that communicate among themselves using radio signals, and a base station where the data can be observed and analyzed. A base station acts as an interface between users and the network [29].

3. **Cloud Computing:** IoT can benefit from the Cloud capabilities and resources to compensate for its technological constraints (e.g., storage, processing, communication). On the other hand, Cloud can benefit from IoT in a more distributive and dynamic manner to deal with the physical world, and for delivering new services in a large number of real-life scenarios. Cloud provides an intermediate layer between the objects and the applications in some cases [30].
4. **Wireless Fidelity (Wi-Fi):** A massive number of devices are connecting to Wi-Fi technology so that the IoT is having an increasing effect on Wi-Fi communications. The requirements of data transmission over Wi-Fi for IoT differs from small, occasional data transfers to a large amount of uninterrupted data [31].
5. **ZigBee:** The ZigBee Alliance creates, maintains, and delivers open, global wireless standards that enable everyday objects to work together and control users' world on the Internet of Things (IoT) [32].

From a business perspective, the IoT is changing the way that organizations are communicating, collaborating, and coordinating daily business processes. The IoT

adopted by the organization is ideal with complex and distributed operations. The Internet of Things allows acquiring accurate data in real-time, enabling a rapid decision-making process, so that the IoT is a crucial fundamental factor for the successful organizational strategy. IoT data is obtained from various kinds of networked sensors in which may be processed by several types of networks, representing that a security challenge. IoT requires highly qualified persons, complicated integration of systems, networks, and applications for the implementation process. This ecosystem contains devices, sensors, networks, cloud storage, and applications, working collectively to help organizations to improve their strategic positioning proactively and reactively. Therefore, the organization must have a distinct idea of what information is vital for businesses, and what type of information they want of the devices, and what is intended to do with the information [33].

IoT uses many different physical devices, applications, and technologies based on the purposes of this technology and where it works. It includes industrial machinery, wearable devices, and monitoring devices. IoT devices communicate together inside a particular network, which involves automated homes, smart cars, health care services, irrigation supply, smart appliances, air conditioning, smart lighting, and smart thermostat. Indeed, most devices that involved in the IoT classify into three different domains of personal usage, industrial fields, and enterprises' utilities. In personal IoT devices, users' connected devices include smart (lighting,

TVs, phones, thermostats, appliances, doorbells, and speakers). While in the industrial fields, the used devices and technologies may vary, encompass smart (factories, metering, grid), security systems, monitoring technologies, and industrial machinery. In addition to the tremendous applications and technologies used in this field, such as transportation, mining, irrigation, and aviation. The IoT devices introduced in enterprises are diversified, ranging from embedded devices with sensors to the cloud platforms. Enterprises are trying to enhance their efficiency, facilitate the business processes while reducing errors and saving time. Therefore, there are numerous of the connected wireless endpoints in enterprises, including many standard workplace objects such as security cameras, locks, office printers and scanners, smart meeting rooms, and many other emerging technologies that allow workers to transmit data with colleagues and help in increasing productivity and saving cost and time.

2.2 Security Threats in IoT

Even though IoT has come a long way since their introduction in the world, various threats remain from the security perspective in IoTs. Owing to the different construction and functionality of different layers of IoTs, the security threats are also different for each layer. Due to this reason, we will analyze the security threats in

each layer separately. As adapted from the works [26], security threats in IoTs classified independently for each layer are as follows:

2.2.1 Application Layer Threats

The application layer contains the applications required for normal operations, which may be compromised in case of security threats. Security issues can result in malfunctioning as well as in shutting down the applications. Some prominent security threats in the application layer are:

1. **Malicious Code Attacks:** There is a distinct possibility that malicious code can attack, such as in the form of a worm, through the internet and attack all the embedded devices running on that system. These attacks can take control of Wi-Fi and other devices.
2. **Tampering of Applications Based on Nodes:** The applications based in the device nodes are susceptible to attackers planting malicious rootkits; this can result in the manipulation of the local environment leading the device to malfunction, such as a temperature sensor giving wrong reading.
3. **Unavailability of Security Patches:** In the continually moving node, software patches might not reach in time and update the security features, which can result in catastrophic consequences such as in systems like nuclear and thermal reactors.

4. **Hacking of Smart Grid:** Attacking into a smart grid or smart meter can increase the threats of robbery or even home violation as the power consumption of a home can give the hacker an idea about when a facility is empty.

2.2.2 Perception Layer Threats

The perception layer contains the sensors which are present at the nodes, so the threats are also at the nodes in the perception layer. Most of the threats related to the tampering of sensors or stealing data. Prominent threats in this layer include [26]:

1. **Eavesdropping:** Due to the wireless communication over the internet between the devices in the perception layer, the devices become susceptible to eavesdropping as the device without monitoring.
2. **Sniffing Attacks:** The sensors recording data present at nodes can leak information in case a malicious device is put near them; this can result in the identification, tracking, and profiling of users, which is a severe security concern leading to violation of privacy.
3. **Noise in Data:** Data being transferred wirelessly over the internet always contains noise in it in the form of wrong or incomplete information. This noise can lead to misinterpretation of data, which can be critical in confidential applications requiring reliable information.

2.2.3 Network Layer Threats

Among other layers, the network layer is most prone to security threats due to large amounts of data it carries, leading to the majority of security concerns with the authentication of data. Some security threats in these in this layer can be summarized as [26]:

1. **Denial of Services (DoS) Attack:** DoS attacks are those in which specific servers and devices are targeted and then bombarded with excess redundant information resulting from the devices unable to provide services to the users as DoS attacks prevent the transfer of data between devices and their sources.
2. **Gateway Attacks:** Gateway attacks can be made through DoS attacks or other attacks in which the connection between sensors and infrastructure over the internet is cut off; this results in no transfer of data or wrong data transmission.
3. **Unauthorized Access:** Some devices are often left unattended as their supervision is not felt necessary all the time or is not possible such as in the case of sensors inside pacemakers. Others violating the security of IoT can access these unattended devices by disguising themselves as authenticated.
4. **Storage Attacks:** Huge amounts of personal data, as well as from sensors and other devices, are stored on the cloud all the time. This data is highly

susceptible to attacks compromising data resulting in loss of illegal use of the data stored online.

5. **Injection of Fake Information:** The network layer in IoT is prone to injection of false information from outside, resulting in malfunction of devices or working of a device in an undesired and inappropriate way.

2.2.4 Physical layer Threats

The physical layer is what is exposed to the environment as well as people making it more prone to external security issues, whether from weather or users. Safeguarding to protect the devices, as well as efficient batteries, are required to make specific physical layers functions properly. Some security issues in physical layer include [26]:

1. **Physical Damage:** As the devices in physical layers are exposed to the outside environment, there is a constant threat of these devices getting damaged. These damaged devices might malfunction or even become vulnerable to other risks when causing the physical device such as sensors or nodes to lose its functions.
2. **Environmental Attacks:** Environmental attacks such as rain, snow, or storm. Remain the biggest threats to the devices in the physical layer as they cannot be controlled. These attacks could lead to other risks, for instance, affecting

sensors until they lose their supposed functionality. What can be done is to improve the physical endurance of the devices to prevent malfunctioning.

3. **Loss of Power:** Devices running on batteries and requiring external power are always at risk of losing power, which causes these devices not to be able to operate normally and results in a denial of service. If power runs out, not only the equipment will stop working, but it will also affect the other devices connected with it.
4. **Hardware Failure:** Hardware failure is something that is always a threat to physical devices. This threat could cause the devices to stop working or sending incorrect data. It also can become more critical when the user is highly dependent on the functionality of the device, as in the case of pacemakers.
5. **Physical Tampering:** It is essential to protect the programmable logic controllers (PLCs) that operate the devices as well as other components as they are also prone to external tampering. The unauthorized person can tamper the device physically, which can result in a malfunction of the device. Therefore, it is critical to protect the PLCs from people's interference.

2.3 Ensuring Security in IoT

The security risks are always present in IoTs at different in different layers depending on the construction of that layer. Just as security threats are various for each layer, schemes to minimize the risks are also separate for each layer depending upon the risk they are facing. Some protection methods against different security risks in each layer adopted from [26] are summarized below:

2.3.1 Application Layer Security

Many security schemes are proposed by different researchers for the security risks present in the application layer. Some solutions include:

1. **A Domain-Specific Metrics (DSM) Approach:** DSM aims to improve the security metrics present in eHealth information by proposing five elements dealing with the security of the information; technology maturity analysis, threat analysis and modeling, requirements establishment, policies and mechanisms, and system behavior [34].
2. **Game Theory:** Game theory is a mathematical technique based on fighting the security attacks by dynamic complex systems by attacking them to ensure better security of the application layer. This tool allows modeling conflict and cooperation between parties (players), who are supposed to defend their benefit (or risk measure). [35].

3. **A Comprehensive and Comparative Metric for Information Security**

(CCM): CCM is a security feature that uses security metrics through a risk assessment approach to improve security. The model quantifies security in terms of incident and asset loss to ensure security [36].

4. **Adaptive Security and Trust Management (ASTM):** ASTM is a dynamic security feature having an ability to adapt to a changing environment to anticipate the unknown threats. It utilizes adaptive learning by changing the internal parameters to sense the dynamic changes in the system [37].

2.3.2 Perception Layer Security

Just as different techniques are present to improve the security in the application layer, some techniques to enhance the security in the perception layer are as follows:

1. **An Adaptive Security Management (ASM) model:** ASM uses a four-step technique to identify a security objective and, after tracking any threats, adapt to the changing environment according to security metrics. The steps in technique involve continuous monitoring, analytics, and predictive function, decision making, and metrics-based adaptive security models [38].
2. **SMC (Self-Managed Cells):** SMC ensures better security by managing and measuring the resources utilizing the ubiquitous computing with defined policy, discovery services, and role [39].

3. **Public Key Infrastructure (PKI):** Public Key Interface is specifically designed to tackle the security threats at nodes. In order to ensure safe transmission of a node, the offspring node is created containing the decryption key hence protecting the node [40].
4. **Cyber Sensors:** Cyber Sensors ensure real-time data acquisition and usage to minimize the chances of data attacks while in the cloud. The data captured by Cyber Sensors are then used later, ensuring real-time data provision [41].
5. **Ambient Assisted Living (AAL):** AAL ensures better security features in IoT, especially for the safety of older people. AAL keeps the user in touch with the outside world using smart objects and sensors such as RFID and NFC [42].

2.3.3 Network Layer Security

Considering that the network layer is most prone to security risks due to communications, the solutions proposed to address these risks also revolve around making the transmission of data more secure. The prominent techniques include:

1. **Security Middleware:** Security Middleware technique is targeted at the provision of secure smart home systems. This technique uses parameters such as Entity Identification, Secure Storage, Security Audit, Data encryption to ensure a safe interface [43].

2. **Authentication and Access Control:** This technique ensures security in the network layer of IoTs by ensuring the integrity of data. It introduces the concept of the Registration Authority, which double-checks the authentication provided by the user each time [44].
3. **The Intelligent Transportation System (ITS):** This technique uses risk analysis to provide security methods and improve standards of efficient performance by addressing the threats to the transportation system. It ensures better security of data at nodes to prevent data at nodes from getting interrupted [45].
4. **Identity Management Framework:** Though this method has not been implemented yet practically, Identity Management Framework authenticates data traveling between device and cloud storage. This technique places an identity manager and service manager on the devices to ensure security [46].

2.3.4 Physical Layer Security

The physical layer is the external layer exposed to the environment with devices in this layer susceptible to physical damages from users as well environment. As the external factors cannot be controlled, there are not many techniques to tackle the security risks in the physical layer. The most prominent scheme in this domain is as:

1. **RFID Tags:** RFID Tags ensure better security in the physical layer by making sure all devices stay interconnected in the physical layer. These RFID

tags can be installed in smart devices in the physical layers to allow rapid communications between interconnected devices and solve the identification issues of objects [47].

2.4 Privacy Issues in IoT

Privacy is a substantial human right that protects people's personal and sensitive information from external interventions, and as a concept, it may differ among people. The privacy term in the IoT is a broad term that refers to using and processing personal information that needs to be protected from exposure in the IoT environment. Also, it defined in [48] as the guarantee that the user has control over their private information. Individuals may not be aware of the massive number of IoT devices they are using and how it may affect privacy risks. While the IoT devices present tremendous opportunities for convenience, they bring privacy risks with a significant influence on people's perception of IoT technology.

Privacy issues in IoT include the following: control personal information, develop the privacy mechanisms and regulations, and base techniques to control user identity [48]. Ziegeldorf's literature review [49] addressed some of the privacy threats on the IoT:

1. **Identification:** The threat of identification is persistent in the IoTs in which an identifier such as an address or name can be associated with an individual,

and then data on that individual can be accessed. Identification is a severe privacy issue that often leads to other privacy threats such as profiling and tracking. This threat is dominant in IoTs currently due to extensive information not only flowing through the systems but also when it is stored, and it becomes more prone to these threats, which can lead to identification. Devices could be identified via fingerprints technology by collecting information about these devices due to the numerous wireless interconnections of daily objects. In addition to recognizing users through RFID technology so that identifying people became feasible through devices around them [51]. Consequently, users may want to remain anonymous, which is why identification may consider as a threat and not a desirable trait.

2. **Localization and Tracking:** Localization and Tracking is a subsequent privacy issue raised after identification has been made. Localization is the continuous determination of a person's location through time and space. A movement of individuals is kept in records, and they are tracked through means such as the Global Positioning System, Internet Traffic Patterns, and Cell Phone Location, this can further lead to severe other privacy violations such as GPS Stalking, Disclosure of private medical records and being continuously monitored.
3. **Profiling:** Profiling utilizes data acquired from other privacy violations leading to compiling of information and creating profiles by correlating

different information gathered. Information collected through profiling is often used for commercial purposes such as advertisements and optimization based on customer demographics and consumer trends. Profiling then leads to privacy violations such as price discrimination, advertisements, social engineering, and erroneous automatic decisions.

4. **Interaction and Presentation:** Privacy Violating Interaction and Presentation is the leaking of confidential information to the unauthorized audience through a public medium. There are many IoT applications, especially in healthcare and transportation, which require intensive interaction with the user, this can result in leaking information gathered through these applications which can be enhanced with unauthorized users. Geneiatakis et al. in [51] analyzed the threat model of a smart home considering two types of adversaries that can act directly or indirectly based on their goals. The internal adversaries include malicious entities that are placed inside the smart home, whereas external adversaries interact only through an Internet connection. Adversaries are trying to access users' information by eavesdropping available communication so they can monitor their behavior or attack them directly. In this way, capturing user's information by the adversaries could profoundly affect their privacy.
5. **Lifecycle Transitions of IoT devices:** There is a chance of privacy violation due to the change of control in the IoT life cycles, which can result in

unwanted disclosure of information. The leaked information can be of all sorts as often photos and videos are observed to be leaked during these transitions posing serious violations to privacy. This threat is most evident during the phase of data collection as the information leaked is the one already collected by the IoT. Besides, the lifecycle transition could influence users' privacy when someone else can infer different things about them. For example, car sensors collect some attributes about drivers' driving habits so that the owner of the data can keep the inferred information and sell it to third parties [52].

6. **Inventory Attack:** Inventory attack refers to the illegal collection of information about the presence and characteristics of personal objects.
7. **Linkage:** Linkage is a privacy threat in which data is revealed using data sources from previously connected systems. Data collected from different sources may lead to loss of context and poor judgment for the users, this can also result in bypassing of security mechanisms which can lead to serious privacy issues such as unauthorized access and leaks of private information.

Kumar and Patel [53] also cover a wide area of privacy issues in the IoT. They divided the privacy concerns into four categories as follows:

1. Devices privacy: unauthorized access to the device may cause leakage of sensitive information. In addition to the location of the devices which can disclose the location of the device holder.
2. Communication privacy: sometimes, data tracking may happen during the transmission of data when data encryption is used and add data to packets, which leads to endangering data.
3. Inventory privacy: the issue in the inventory is that personal information is tied with real identity, which can pose a risk to user privacy.
4. Processing Privacy: personal data should be processed in a way that achieves the required purposes and should remain reserved while there is no explicit permission from the owner of that data to be disclosed.

2.5 Privacy Protection

Privacy issues are mostly originated due to operations over the internet, exposing confidential information to the attackers. In the case of IoT, not only are the users exposed to privacy violations, but everyone present in the environment is also exposed to risks. Moreover, due to the proliferation of IoT applications at various locations, users need protection for their personal and confidential information

associated with their locations, behavior, and communication with others. Therefore, users' privacy should be preserved [55].

In [56], authors address a method that allows users to control their collected and accessed personal data in addition to knowing who is collecting and accessing that data and when such processes happen. All of these happen via a proposed protocol called a user-controlled privacy-preserved access control that depends on context-aware k-anonymity privacy policy.

In [57], there are two categories extracted from the traditional privacy techniques: Discretionary Access, which discussed the minimum privacy risks to avoid the disclosure or copying of confidential information, and Limited Access, which is seeking to minimize the security access to prevent malicious unauthorized attacks.

In [58], the author analyzes the privacy risks that happen when the static domain name is allocated to a particular IoT device and propose privacy protection enhanced DNS (Domain Name System) for intelligent devices to authenticate the authentic users' identity and reject the illegitimate access to the devices. The author in [59] proposes a privacy management scheme that is aimed at limiting private data disclosure and sensitive content analysis. This scheme allows users to consider the risks of sharing sensitive information and attempts to originate a robust system for sensitivity detection that measures the quantity of the privacy content of the information, in addition to that the proposed strategy is generic, which allows being adaptable in various time-series sensor data-based applications. In [60], the authors

introduce and survey challenges from three critical issues related to data analysis, trading, and aggregation for security-critical and privacy-sensitive data, and introduce privacy-preserving mechanisms in the IoT to improve the privacy and fulfill the required functional requirements. However, to protect the location privacy of users with minimizing the cost of obtaining desired services is a new strategy that integrated from the cache scheme and k-anonymous proposed by the authors in [61].

Owing to the importance of protecting privacy in IoT, numerous techniques are already in implementation to protect various privacy attacks. These techniques can be mainly classified into four categories; authentication and authorization, edge computing and plug-in architectures, data anonymization, digital forgetting, and data summarization aimed at protecting each aspect of privacy. According to [62], the most prominent privacy protection schemes in each category of a privacy issue is summarized below:

2.5.1 Authentication and Authorization

Authentication and Authorization based privacy risks needs to be addressed to make sure that an unauthorized person cannot access the private information of users flowing through the servers, ensuring protection against data misuse. Prominent privacy-enhancing techniques in the domain of authenticating and authorization are as follows:

1. **Lightweight Authentication:** Lightweight authentication techniques ensure authentication in constrained environments by utilizing a method of encryption based on XOR operations.
2. **Device Fingerprinting:** Device fingerprinting is a privacy protection technique which uses the method of giving each device a unique fingerprint that contains the gathered information about the hardware and software of that device, this ensures authentication of devices by verifying that the generated message belongs to particular object and the sender of the message is legitimate [63].
3. **PAuth Key Protocol:** PAuth Key Protocol is a privacy protection scheme specially designed for IoT with resource constraints. In this technique, end to end verification is ensured by two phases: the registration phase of users for acquiring cryptographic credentials and authentication phase in communication [64].
4. **SmartOrBAC:** SmartOrBAC is a context-aware authentication technique having the ability to accommodate IoT network requirements. This scheme uses real-time IoT context to make authentication decisions [65].

2.5.2 Edge Computing and Plug-In Architectures

A class of authentication and privacy techniques based on edge computing and plug-in architectures is highly popular nowadays. Various schemes are present in this category among which the most prominent ones include:

1. **Edge Computing Paradigm:** Edge Computing Paradigm is a privacy ensuring technique in which data processing and storing occur in the network edge that provides an entry point into central networks. Due to the generation of data at the edge, issues such as latency, security, and user privacy are substantially resolved [66].
2. **Privacy-Aware System (pawS):** PawS is a system specifically designed to tackle the privacy challenges by ensuring data stays confidential. It uses data processing and collection tools which notify users what is being processed and collected, ensuring privacy [67].
3. **Sentry@HOME:** Sentry@HOME is specifically designed to protect privacy in Smart Homes. A user-centric approach is adopted in this framework, which disseminates a users' private data according to privacy policies defined by them [68].

2.5.3 Data Anonymization

Data anonymization is a privacy protection technique in which identifiable information is removed to avoid leading to people being identified by data. Data Anonymization is achieved through various strategies, among which the most prominent ones include:

1. **Deep Risk Analysis:** It is a technique to pull data anonymization through deep risk analysis, which can be done by implementing an authentication algorithm having the ability to verify the source of updated files by using a cryptographic mechanism.
2. **Identification-Based Key Sharing:** Identification-Based Key Sharing is a privacy-ensuring technique providing data anonymization through mutual authentication and encryption of data communication. This technology provides an anonymization technique by using identification information of a user or a device as a public key, which allows small-section data to be disclosed through the use of layers of meshes on a map to utilize the positional data[69].

2.5.4 Digital Forgetting and Data Summarization

The last set of techniques that target to ensure maximum privacy in IoTs are the Digital Forgetting and Data Summarization techniques. The process of removing all

the copies of datasets used during communication is called data forgetting, whereas data summarization is the provision of high-end abstraction, which hides specific details from data and reduces its size [70]. With techniques such as digital forgetting and data summarization, the user can become more satisfied as data is disposed-off, and his privacy is secured.

Data Summarization can be divided into two main categories based on the nature of data transmission and recording [62]. These categories are:

1. Temporal Summarization: In temporal summarization, data is collected as a function of time. For example, if data was being collected at per second rate, after temporal summarization, it will be collected after per hour rate. Researchers in [71] addressed a temporal strategy for privacy-preserving based on the time-dependent priority queue, that tackles the random delays problems and time-driven model mechanisms, nevertheless, this work is deficient in privacy analysis and data encryption.
2. Spatial Summarization: In spatial summarization, data is collected as a function of location. For example, if data was being recorded at all locations based on GPS, after Spatial Summarization, it will be gathered at particular zip codes only.

2.6 Privacy Protection in Layers of IoT

Just as security protection schemes were analyzed from the perspective of each layer depending on its applications and structure, the privacy protection techniques can also be observed through the perspective of layers considering different techniques in each layer. As physical layers contain hardware components, this layer is less susceptible to privacy attacks and more prone to security attacks due to which there are not many techniques aimed at solving privacy issues in Physical Layer. The most prominent privacy protection techniques in each layer as adapted from [62] can be summarized as:

2.6.1 Privacy Protection in Application Layer

In the application layer, privacy concerns are present in two parts: in the support layer and service layer. The support layer is responsible for edge computing and analytical services, whereas the service layer is responsible for providing the necessary support for IoT to function. Various techniques to ensure privacy in Application Layer include:

1. **Preference Based Privacy Protection:** Preference-Based Privacy Protection is a technique aimed at reducing the issues in data privacy. In the scheme, a third-party entity is used for the evaluation of privacy preferences and

conveys them to the service provider to ensure the highest privacy levels based on preferences set [72].

2. **Privacy Awareness:** The users are made aware of the potential privacy risks while using their devices. Users are conveyed and made aware of private data collection, potential risks, and safe handling of IoTs. In [73], authors have addressed some mechanisms for privacy protection such as awareness and control to improving user's privacy. Moreover, a management system for users' data was proposed in [74] that combines blockchain technology with an off-blockchain storage solution to enable users to be aware of data that is collected about them by the providers.
3. **Security Management:** Security management includes applying protective measures to preserve privacy, such as by managing passwords and securing physical information.
4. **Cryptography:** Cryptography is an effective privacy protection technique utilizing and implementing technologies such as fingerprints, digital watermarking, anonymous authentication, and homomorphic cryptography. A distributed target-driven anonymous authentication protocol for IoT applications is proposed in [75] to authenticate users anonymously. This protocol depends on a multi-show credentials system. Whereas in [76], a standard format to describe data in IoT has been proposed, which includes personal information. This work considered using encryption, anonymity,

minimize data, authentication for privacy protection. In [77], a system proposed based on public-key solutions that protect data in IoT devices by using IoT gateway. It applies data encryption, user access control, and communication security mechanisms after it captured data to achieve the essential privacy requirements.

5. **Key agreements:** Key agreements protect any potential privacy violations in the application layer by incorporating both symmetric as well as asymmetric cryptosystems and certified transmission technology. Authors in the work of Nguyen et al. [78] propose an analysis of the key-bootstrapping cryptographic techniques in IoT. They analyze the key establishment and authentications mechanisms based on asymmetric schemes and symmetric pre-distributed keys. Further, biometric-based key agreement protocol is used in IoT devices for privacy-preserving, such as in [79], researchers use unique biometric data such as, EKG data that obtained from the owner of data to establish cryptographic keys for privacy purposes

2.6.2 Privacy Protection in Network Layer

The network layer contains data being transmitted all the time from one host to the other located in different networks, in addition to that it is responsible for packet routing. Due to the wireless transmission taking place over the internet, this layer is

severely exposed to the risks of data stealing and compromise of private information.

Due to this reason, some of the privacy features adopted in this layer also ensure data privacy above other things. However, in the direction of providing security and privacy in The IoT communication, [80] describes a group of trust-enhancing security components for the IoT infrastructures.

Furthermore, some significant techniques ensuring privacy in network layer are as follows:

1. **End-To-End Authentication:** End to End authentication is set up to ensure the safe and confidential transmission of data from one to another. End to End authentication is achieved by employing methods such as key agreement, Public-Key interface, and secure routing. Bonetto et al. [81] present a secure end-to-end communication scheme between Information and Communication Technology (ICT) devices, which includes all technologies for the communication of information, and Internet of Things (IoT) devices, by recommending that using trusted unconstrained devices to unload computational processes. In addition to the work of Weber et al. [82], which proposes an approach for identity and access management for the Internet that includes users, services, and objects. This approach is based on using trusted personal devices (Minimal Entity); it focuses on end-to-end secure communication and user privacy concerns. Another work that focuses on end-users ' privacy-preserving in the IoT is presented in the work of Henze et

al. [83], which addressed a user-driven privacy enforcement strategy for cloud-based services. Further, the researchers in [84] have suggested a privacy-preserving aggregation protocol (PAGIoT) for IoT setting that allows multi-attribute aggregation in a set of elements with more focus on privacy-protecting value correlation.

2. **Network Virtualization:** Network Virtualization is a technique used to minimize the risks of inappropriate and unauthorized operation in the network layer. It achieves this purpose by reducing the network management complexity hence reducing the likelihood of privacy violation.
3. **IPv6 Protocol:** IPv6 Protocol is carried out in the network layer to protect data from being mishandled or tampered. It employs inherited security mechanisms in network layers and enables their support for successful defense [85]. Further, according to [86], IPv6 provides for privacy by automatically employing random arrangement for the suffix of the IPv6 address to hide the MAC address or any identifier number when connecting to the Internet.

2.6.3 Privacy Protection in Perception Layer

As the perception layer contains all the sensors recording data, it is necessary to protect it from privacy violations to avoid misuse of data being recorded by sensors.

Some privacy risks in this layer include node capture, malicious information, and node authentication problem which are addressed by techniques such as:

1. **Selective RFID Jamming:** Selective RFID jamming is a privacy ensuring technique based on low-cost tags. It prevents an IoT from privacy leaks, thus protecting user's privacy by preventing open and unauthorized access [87].
2. **Nonlinear Key Algorithm for Data Encryption:** Nonlinear Key Algorithm secure data exchange and guarantees safe transmission of data from one end to another. This algorithm provides data encryption using an algorithm based on displaced calculation requiring very low computational power to provide not only high security but also fast transmission [88]. In the direction of using lightweight encryption to utilize cryptographic algorithms, the work in [89] has presented a method for IoT devices to protect users' end-to-end communications from distributed DoS attacks. Li et al. [90] proposed a lightweight authentication protocol using a public key encryption method for smart cities' application protection.
3. **Secure channel using IPSec:** Implementation of the secure channel using IPSec ensures data authentication as well as data encryption [91]. IPSec is very efficient in ensuring privacy, even outperforming IEEE 802.15.4 link-layer security in IoTs [92].
4. **Cryptography:** Just as cryptography finds its applications in ensuring privacy in the application layer, cryptography is used to protect privacy in the

perception layer by offering confidentiality, authenticity, and data integrity.

The protocol used in cryptography for the perception layer includes digital signatures and unique hash values. Boneh et al. [93] addressed a public key encryption scheme with keyword search (PEKS), based on public-key cryptography to tackle the problem of secret Key distribution complexity. This searchable encryption scheme allows users to retrieve encrypted data. To protect the data, researchers in [94] apply Diffie Hellman key exchange and hashing in smart homes to protect the privacy in decentralized content.

Many researchers are engaged in exploring different strategies and methods to ensure privacy, such as the authors in [95] who differentiated between the definition of privacy and security in their work, in addition, to pointed out some various techniques that used to achieve the privacy requirements with mentioning some advantages and disadvantages of addressed methods.

2.7 Privacy-by-Design Principle

In a vision of the future where everything is connected, the data may be collected from anywhere without users being aware. Therefore, researchers and developers in the field of IoT should consider the Privacy-by-Design principle which is a security

engineering strategy that considers privacy requirements as organizational goals in business and identification processes [96], it has followed seven keys principles:[97]

1. Take proactive measures that prevent privacy issues in a design phase.
2. Protect the privacy automatically in any business processes, as a default.
3. Embed the privacy into the design.
4. Ensure full functionality in a positive-sum "win-win" way at the end of a communication.
5. Ensure end-to-end security.
6. Ensure that all components and operations are visible and transparent to users.
7. Respect user privacy.

Privacy-by-Design protects privacy in IoT by focusing on IoT sensors, legal regulations, cloud computing, and analyzing massive data [98].

2.8 Summary

This chapter has presented an overview of IoT, its definition, its history, and its applications also highlighted the architecture design of IoT, two different architectures have been outlined: IoT Forum Architecture and International Telecommunication Union (ITU) Architecture. Furthermore, the security threats and privacy issues in IoT have been addressed in this chapter in order to perceive the

privacy challenges that may pose a threat to the users' perception of the IoT devices.

The final part in this chapter discussed some techniques that have been proposed and used to ensure security and protect privacy in IoT which is the central part in the literature review that enable us to know the gap in existing solutions and try to find a solution that contributes to addressing the privacy issues.

Chapter 3

Design and Methodology

This chapter addresses the research questions, which aims to evaluate an independent web interface for IoT users to enable them to manage their IoT devices from anywhere at any time and determine their privacy preferences for each specific device. This chapter also explains the proposed website as well as its structures, functions, and design. Additionally, this chapter highlights some of the previous research in the same area and compares them with our proposed solution.

3.1 Introduction

According to Gartner's forecast [1], 20.4 billion connected objects will be in use worldwide by 2020. Whereas, these massive numbers of connected devices are invading our surroundings and capturing our sensitive information without our knowledge nor our permission. Therefore, the IoT users may need to find a way that enables them to view and manage their captured data by IoT devices. Accordingly, we believe that this can lead to the improvement of their privacy perceptions in IoT devices. Therefore, the idea of establishing a user-friendly “Web-Based User-Interface for the Internet of Things Devices” comes in, which will enable IoT users

to control and manage their IoT devices. In the simplest terms, this is the means by which a user and its IoT devices interact in order to privacy-preserving.

3.2 Related Work

In the same direction, many researchers have proposed solutions to allow IoT users to manage their devices via a web page or an application. In [99], Piyare addressed a low cost, flexible, and Web-server-based solution to home control. Piyare's proposal was based on using an embedded micro-web server and IP connectivity to access and control devices via an Android-based Smartphone app, RESTful based Web services were used as an interoperable application layer for communication. The proposed system supported both Wi-Fi connection and mobile-cellular networks. However, Piyare's system is only for switching and controlling home appliances and devices, it is an Android-based app that can work only by using Android Smartphone or Android Tablet, and the system does not focus on the user's privacy. Another work was proposed by Dhake, et al. [100] that utilized ASP.NET to create the web server that could control the smart home through it and interact with devices remotely using Android Smartphones. The proposal used the ATmega2560 Arduino version. The Intel Galileo development board with built-in Wi-Fi card port acted as a web server; it provides voice command functionalities, security, and save energy as well. On the other hand, this system is an Android-based

app that works only on Android smartphones. In [101], Shrestha et al. addressed a technology that used as a smart home system, which could be controlled by both Android applications in smartphones and a web page. The proposed system was enabling people to control smart home appliances, and it supported Arduino Uno and Wi-Fi. This technology aims to protect security by providing authentication for users. However, this system is an Android-based that controls Smart home only.

On the other hand, the previously mentioned proposed systems may have some limitations. For example, most of the solutions that were proposed were to control smart home devices and appliances only. These solutions were designed to control specific devices; thus, they may not be able to control or manage other IoT devices that are in another different application. In addition, they are proposed for controlling and monitoring purposes rather than privacy-preserving for IoT users.

Furthermore, there are various platforms (applications) that aim to provide a management platform for IoT devices. For example, the RestThing [102] is a Representational State Transfer (REST)-based platform that was designed to enable developers to build REST-based applications, combining physical and technological resources so that devices and information are both represented and controlled by a REST interface. Moreover, in [103], a web-based paradigm (EcoDiF) has been introduced in which it combines physical devices with applications and users with external web services. It aims to offer a platform that provides real-time data monitoring and visualizing. Both platforms combine physical devices with IoT

networks and use web services to control devices; however, both are mostly for IoT devices monitoring purposes, and the EcoDiF system has a limitation in its Applications Module, which requires codifying by hand the programming logic of the EMMML scripts regarding the applications. Another platform has been addressed in [104], Silva et al., proposed system management for devices and networks in IoT with user interface (M4DN.IoT). This proposed solution provides information about connected devices and networks. It can be used from any device, such as smartphones, computers, and tablets, and it supports both automatic IoT networks management and user interface. Nevertheless, all of the previously mentioned platforms were proposed to enable the user to monitor IoT devices through these platforms with no focusing on user's privacy-preserving when they are using Smart devices that can capture user's sensitive information. Therefore, we believe that there is still a need to propose a system that enables IoT users to manage and control their IoT devices to protect their personal information and preserve their privacy when using IoT devices.

3.3 The Proposed Platform

In this study, we have proposed a system that aims at finding a solution for some of the concerns that are arising regarding the privacy perspective and the lack of a user interface in some of IoT devices. Since there is an enormous number of connected devices and embedded sensors in objects that collect various types of people's

information, such as personal information, the collection of data has become more accessible, and it can be achieved without people's awareness. Hence, many of the IoT services may be avoided by many people due to the invisible collection and processing of data. The proposed solution also aims to improve users' perceptions of IoT devices and their privacy when using IoT devices. The proposal is a web-based User Interface that is like a web app, where it can be accessed by using a particular URL (<http://iotprivacycontrol.com/>). However, this web app has specific functionalities that can be seen in; controlling an IoT device remotely, accessing information about an IoT device (i.e., device status), controlling what information can be collected from an IoT device, and setting some privacy preferences for a specific IoT device. The web app can be accessed via different operating systems such as iOS, Android, and the reason behind that is that users will be using a web browser instead of actually downloading a given application which means the web app does not need a specific operating system or a separate software development. Also, because users do not need to download an application, accessing the website may be easier for them, which can be done by providing them with the URL link. This web app may allow IoT users to access, control, and interact with their IoT devices.

The significant features of the proposed web app are:

1. The ability to access information (by users) about the IoT connected devices through the website such as a device's status (Devices should

be connected to the web app by the users, and then they will be able to access the device information).

2. The ability to control different IoT connected devices remotely such as switching on/off the device, and scheduling tasks for a specific device to a particular time via the website, at various locations such as homes, workplaces, and vehicles.
3. The ability to control and manage the collected information by IoT devices about the users via the website, which can enable them to monitor their data. For example, users can control what a particular device can collect information about them, and they can set their privacy preferences for each device based on the device location.
4. The ability to view operations of the connected devices in real time, such as pending, and execution.
5. The ability to manage devices' software, and manage devices' permissions, e.g. change password.

Since some of the previously mentioned proposed systems may have some limitations, for example, some of the solutions that were proposed to control smart home devices and appliances only or were designed to control specific devices; thus, they may not be able to control or manage other IoT devices that are in another different domain. Besides, some solutions require some level of technical skills from

users, and some of them work with a specific operating system or on specific devices. Moreover, some of the previous IoT device management is proposed for controlling and monitoring purposes only and they do not focus on IoT user's privacy-preserving. Whereas our proposed website is intended to focus on solving these weaknesses in previous work with more focusing on IoT user's privacy-protecting.

3.3.1 Detailed Description

The environment of the Website “Web-based User Interface for IoT device management” includes IoT devices, user interface (WordPress website), Function request module, Function execution module, and database. Moreover, it uses Node/JavaScript language to extend the WordPress user experience. In the proposed paradigm, the IoT users communicate with IoT devices through a standardized Application Programming Interface (API) via the website. Therefore, each device needs to be connected to the web app by a separate Application Programming Interface (API), (as all IoT devices are controlled by the API/Web Services interface provided by their respective creators, and they come with their unique set of capabilities, protocols, and functionalities to exchange data), which enables the website to be integrated with the IoT device's operating system to call the specific trigger with the device, where the IoT users from the website will manage the trigger data. When the user clicks on a particular service from the web app, then the API

will call for the specific device to expose data that enables those connected devices to exchange data with the web app, besides, to allow the web app to control the IoT device. The website contains information about IoT devices and provides a user-interface through which IoT devices can be managed and controlled. By standardizing interactions between the website and IoT devices, IoT devices can be managed from one platform, without requiring a separate application for each IoT device.

The function request module communicates with an IoT device via the Internet. Then the IoT device answers with a response displaying the functionalities that are related to that device. The function request module receives the response from the IoT device. The IoT device can return functions that are available on the device through the web response. The function request module stores the information about the IoT device and the functionalities in the MySQL database for the later recalling by the website. After that, the function execution module sends an execution request to the IoT device. An execution request identifies the function that the IoT device should execute. The execution request is a human, machine-readable text which is generated by using JSON strings. The function execution module sends the formatted network request to the IoT device, which consists of the JSON-format string. The particular action displays on the website (User Interface).

A web app is connected to the IoT devices from where the user can log in with confidential credentials and can manage the IoT connected devices, which can be

controlled from anywhere via the web app by using the Internet. Users can monitor the data that is captured from a particular connected device and set their privacy preferences for each connected device based on the device location. Therefore, users should create an account on the website for the authentication purposes and log into their account to utilize the website and add the IoT devices that will be managed via the website. The website provides analytics services to leverage the data collected, and it displays the collected historical data about functionalities requests and executions. For each IoT device, a user can access historical and analytical data for that particular IoT device. The website displays a list of registered IoT devices according to their categories. The database is a MySQL database that provides enough storage capacity to store the needed data and supporting structures. IoT users also can use Mobile devices or computers to connect their IoT devices to the website via the Internet or other public networks to manage and control them. In order to connect the IoT devices to the web app, users will enter the IoT device's details on the web app after they choose the correct category for the device, and then they can access information about the connected devices.

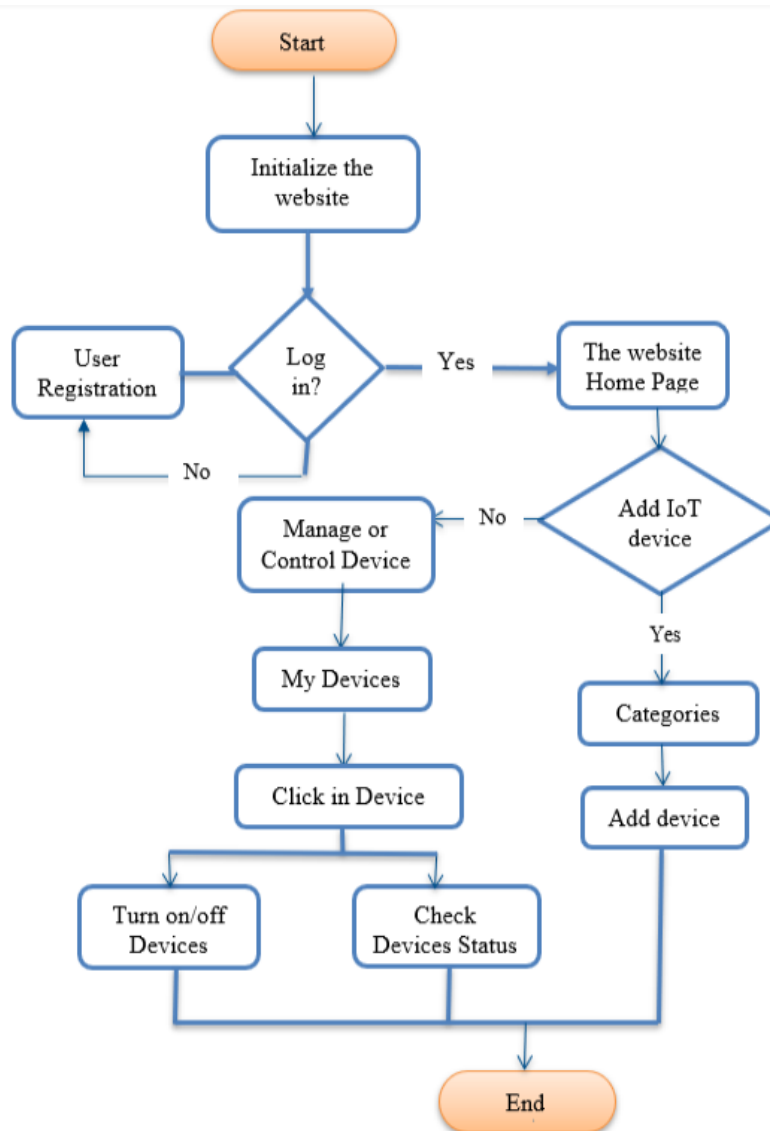


Figure 2 - Dataflow Diagram of the Website

3.4 The Proposed Prototype

At this stage, the descriptions mentioned above are not all implemented since there is a need to integrate APIs for IoT devices to connect them directly to the web app. Whereas, each device has a distinct set of capabilities, protocols, commands, and functionalities, which are used to communicate a message between the device and the platform. Therefore, there is a need to integrate a related API for each device, which makes it harder to implement all procedures in this stage. However, a prototype was created that can be used to demonstrate and evaluate the concept of a “Web App” which can manage the IoT devices for the privacy-preserving.

3.4.1 The Prototype Website (User-Interface) Structure

The website has been created by using the WordPress program (an open source) as a Content Management System (CMS) that includes plugin architecture and template system features. It is accessible by entering its URL address (<http://iotprivacycontrol.com/>). The reasons behind using the WordPress program are it is compatibility with various search engines, and the ability to provide various capabilities for our needs, such as upgrading the site easily and getting the benefit of responsive web design. The web app contains a login system for user authentication purposes that allows users to login with confidential credentials to only allow authenticated users to use the website and protect its resources from

unauthorized users. The web app currently contains three main pages, which are Home page where users can navigate to other pages, Categories page where users can select the specific category of their IoT devices, and Account page where users can access/login to their accounts. The website is real-time monitoring, a responsive web app that works on every device that can access the internet (e.g., mobiles, tablets, and desktops), and implements for real-time users' experience. The web app structure can be seen in the following diagram:

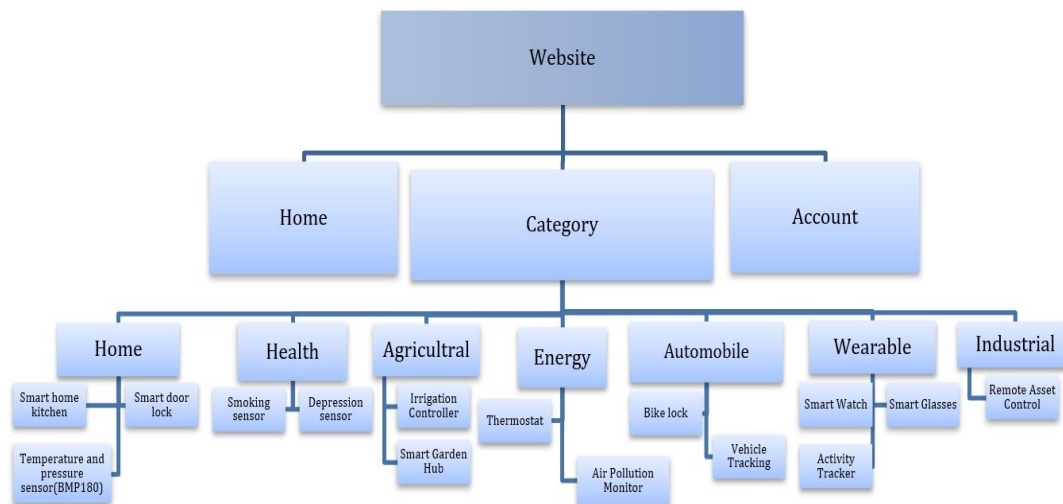


Figure 3 - The Web App Structure

3.4.1.1 Home Page

The first page is a Home page that includes a brief statement about the page that gives new visitors an instant understanding of the site. The navigation bar can be found on the top of the home page, and it includes links to each of the main sections

of the website. The home page also includes a "back to the top" button at the bottom of the page that can be helpful for visitors to return to the menu links.

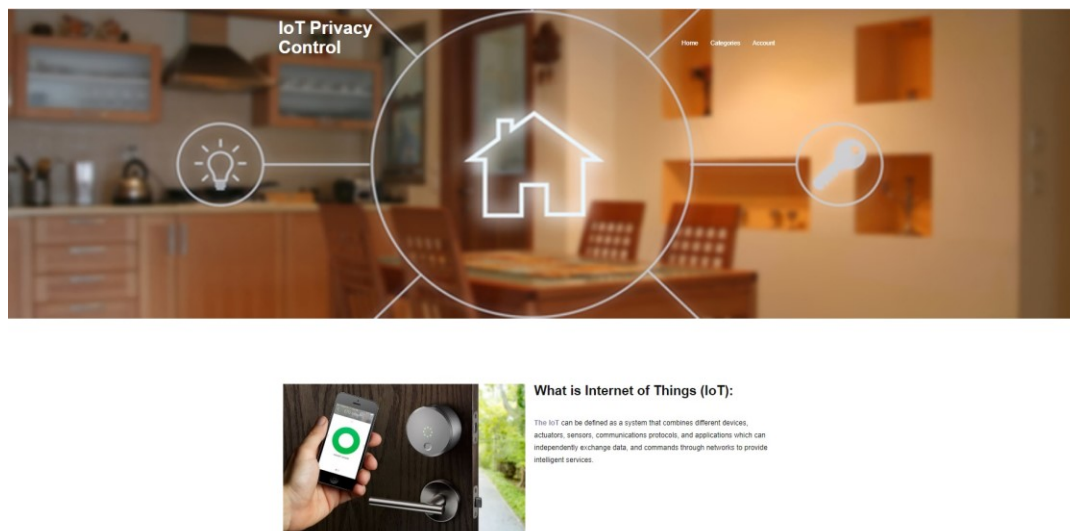


Figure 4 - Home Page

3.4.1.2 Categories Page

The second page is the Categories page, which contains seven categories (IoT applications), the categories are home, health, agricultural, automobile, wearable, energy, and industrial. These categories were selected based on several factors, including importance to user's daily life, and their coverage on a large number of IoT devices and sensors. Each category after clicking on it will lead to another page that contains IoT devices that fall under that category, which many of these devices are used by many of IoT users such as, Smart Watch, Smart Glasses, and Smart Home

Kitchen. The User must add the IoT devices that will be managed via the website. In this stage of the website, due to the APIs integration that have been done with these displayed devices, users only can connect their IoT devices and add them to their account based on the currently available categories and listed devices.



Figure 5 – Categories Page

3.4.1.3 Account Page

The last page is the Account page (user registration feature) that allows users to have an account by signing up as a new user with the following required information: Email address, and Password, and then they can log in with their credentials at any time from any device.

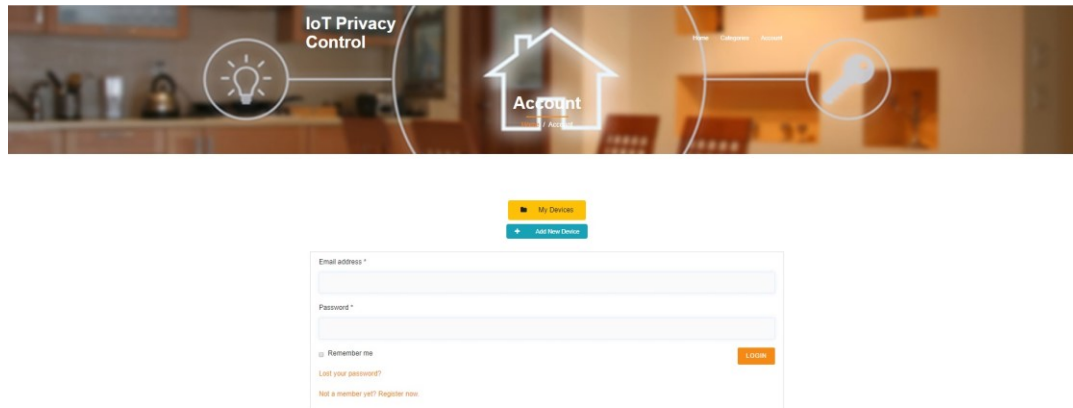
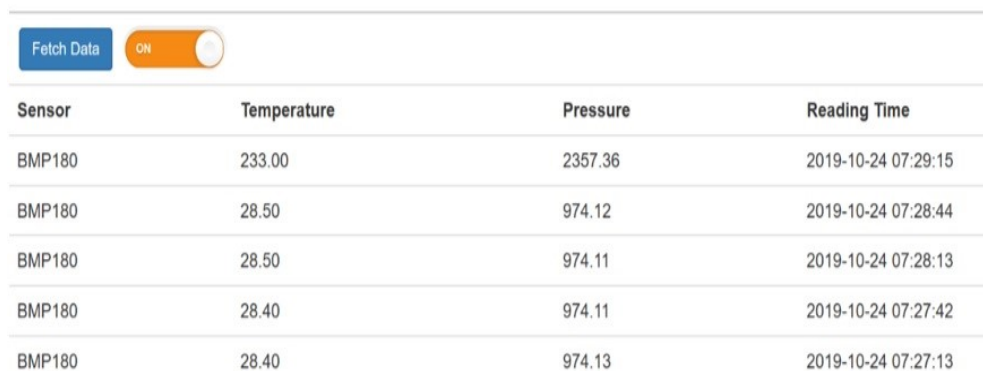


Figure 6 – Account Page

3.4.2 The Prototype IoT Device

After the website has been created, there was a need to connect a given IoT device to the website in order to experience the website's features. Therefore, the IoT device has been created and used in this study. The IoT device has been built by using BMP180 temperature and pressure sensor connected to an ESP32 controller board that is programmed with Arduino IDE, using a PHP script to insert data into MySQL that stores readings and display them on the website, in addition to using a Mobile hotspot to attach the device to the website. The BMP180 has been chosen because it has a low-cost, and it is used to measure real-time temperature and pressure, also to estimate the altitude that affects the pressure. Moreover, the ESP32 has been chosen because it is a low power system with integrated Wi-Fi; it is universally used in IoT

applications. The wires that are used for wiring the BMP180 to the ESP32, the I2C pins are GPIO 22: SCL (SCK), and GPIO 21: SDA (SDI). Consequently, all the values from the BMP180 sensor, such as temperature and pressure of that particular area, will be shown on the website using the MySQL database. Whatever the sensors capture will be formatted and sent to the server for storage and processing to be shown in a human-readable format and not just raw data. Our website will display the BMP180 sensor readings and timestamps from the database to allow data visualization on the website by accessing it from anywhere, as shown in Figure 6.



Sensor	Temperature	Pressure	Reading Time
BMP180	233.00	2357.36	2019-10-24 07:29:15
BMP180	28.50	974.12	2019-10-24 07:28:44
BMP180	28.50	974.11	2019-10-24 07:28:13
BMP180	28.40	974.11	2019-10-24 07:27:42
BMP180	28.40	974.13	2019-10-24 07:27:13

Figure 7 – Data Visualization from BMP180 Sensor

3.4.3. The Website Weaknesses

Since each IoT device needs to be connected to the website by a separate Application Programming Interface (API), the website is not able to manage any IoT device until its API is implemented which the user cannot do themselves.

3.4.4 Expected Feedback

Not only should the website play an essential role in changing users' perceptions of IoT devices, but it should also play a key role in users' daily lives by making them convenient and comfortable. Once the users experience the website, they will be able to see the captured data by the connected IoT device (BMP180 sensor), so they can have the optimal idea about IoT devices' website management, which can be accessed from anywhere at any time. The website will provide the users with a user interface that enables them to interact with the IoT connected devices and navigate between IoT applications to add their IoT devices from them to the website.

3.5 Summary

This chapter explains the proposed solution for the IoT devices management website, its focus, design, and structure. It presents the main feature of the website that enables IoT users to control and manage their devices from any location at any time in an effortless way. Besides, some related work has been addressed and compared to our proposed website in terms of addressing the previous work limitations and aiming to overcome them in our proposal. Finally, the detailed description of the website and its functionalities have been addressed with the expected feedback that should user get after experiencing the website.

Chapter 4

User Study and Findings

In this chapter we will outline the study design that we employed to test our study's hypotheses, it describes the participants of the study, the instruments used, the procedure of data collection, and statistical tests that have been used for data analysis and interpretation. Finally, this chapter outlines the study limitations. The study was approved by the Florida Institute of Technology Institutional Review Board (IRB number 19-175).

4.1 General Purpose

The project is a web-based user interface that enables IoT users to connect their IoT devices to it, then allows them to manage and control the connected devices. The purpose of this study is to examine the implementation of the prototype that allows IoT users to control their IoT devices and protect their privacy in the IoT environment.

4.1.1 Specific Aims

1. To understand the privacy concerns that are related to the IoT environment and understand how to confront these issues.
2. To provide featured means to preserve IoT users' privacy by providing them with a prototype implementation of a web-based user interface that enables IoT users to connect various types of their IoT devices to that interface and control them.
3. To provide an easy to use website, for IoT users that can be adapted by any of the IoT domains (e.g., smart workplace, smart homes, security & surveillance, and mobile devices).
4. To validate the objectives mentioned above in real-time activities in different IoT domains.
5. To raise people's awareness of their privacy when using IoT devices and change their perceptions about their privacy when using IoT devices.

4.1.2 Research questions

Q 1- When using smart devices, is privacy or convenience more important for users?

Q 2- Does the amount of IoT device use by users have an effect on the importance of the following actions to them: "allowing users to control what information is collected about them, informing users when their information is collected, and

requesting users' permission to collect their information”, to protect their personal information that is captured by IoT devices?

Q 3- To what extent does offering an independent web interface, which does not require a specific operating system or separate software development for IoT devices management, gain users' satisfaction?

4.1.3 Hypotheses

H 1- When users use smart devices, privacy is more important to them than convenience.

H 2- The users' usage amount of IoT devices does not affect the importance of the following actions to them: allowing users to control what information is collected about them, informing them when their personal information is collected, and requesting their permission to collect their information before it is collected, in terms of protecting their information that is captured by IoT devices.

H 3- When the participants experience the web-user interface (The prototype of our website), they will be satisfied with the website organization, ease of the website navigation, and the user interface.

4.2 Study Design Description: Instruments and Methods

The following methods were used when conducting this research:

- Experimental study: the participants in this study used the website (Web-based User Interface for IoT Devices) to examine its functionality, usability, interface, and performance. The prototype can be seen interacted with any device at any location via a link (<http://iotprivacycontrol.com/>) of the website, which has been tested to evaluate quantitatively the participants' performance in the experimental group.
- Survey: filled online using Survey Monkey. The survey included questions about privacy (in general and IoT privacy), the website, and user's opinions about the website to assess the participants' perceptions of their privacy when using IoT devices.
 1. Users began by reading and agreeing to the Informed Consent form.
 2. Users were instructed to browse to (<http://iotprivacycontrol.com/>) to the website under study using any device.
 3. The participants logged in to the website as a particular user that the participants assumed it was their account to give them an idea about user registration used for authentication purposes.
 4. Users asked to complete the following tasks:

- A. Discover how many devices they have connected to the website.
- B. Add a smart door lock to their account.
- C. Obtain information about the data sent by the BMP180 sensor (IoT connected device).

The above tasks were chosen to mimic the basic functionalities of the website.

5. Users completed the questionnaire about their experience with using the website, as well as their subjective impressions about the privacy risks associated with the website. Once the questionnaire was completed, the users have been thanked, and the study was completed.

4.3 Participants Characteristics

Human subjects are involved in this study by requesting them to use the website and answer some questions through the questionnaire. Participants had to be 18 years of age or older, and no other inclusion criteria applied. We welcomed participants of any gender, ethnic background, and health/treatment status in which minorities and women were not excluded. There were no physical, psychological, social, legal, or other risks to the study participants.

A total of 45 participants participated in the study. Out of 45 participants who responded to the question of consent to take part in this survey, 43 participants agreed

to answer the survey; 2 did not agree to answer the survey, in which their surveys were closed directly, and their data was removed. The 43 participants were allowed to skip questions for their convenience.

4.3.1 Sampling Technique used

The participants recruited using convenience and snowball sampling methods. Participants were not compensated for their participation.

4.4 Data Acquisition

We asked each participant to do the tasks and answer their related three questions in the survey and then asked them to answer demographic questions, after that we exposed the participant to different scenarios and asked them to answer the questions about them. Scenarios are hypothetical situations in specified circumstances that can give them a visualization of IoT devices, data collection, and privacy.

We hypothesized some factors that could influence individuals' privacy perceptions:

- The type of data collected.
- The collection of users' data without their knowledge.
- The location where the data is collected.
- The control of data collected.

- Type of devices that collect data.
- The retention time of data collected.
- The control of devices.

The reason behind studying these factors is to determine the contextual nuance between IoT users' and how they affect their perceptions of privacy when using IoT devices. Each scenario includes a number of these factors. The following is an example of our scenarios: "Assume you are at your friend's house and they have a security camera which is recording audio and video that is kept for one week. How important to you are each of the following actions in terms of protecting your personal information that is captured by that IoT device". This scenario contains some factors such as the location of data (friend's house), type of the device (security camera), type of data collected (audio and video recordings), and the retention period (one week). Each scenario has some questions related to it, that can elicit the information about their perception of privacy. In addition, we asked questions about how concerned they are of their privacy when using IoT devices and how they want to manage their devices.

4.4.1 Structure of the Survey

Our survey was divided into five parts.

1. Demographic Information: we collected the participants' age, the highest level of education, and what IoT devices they have.
2. Participants' understanding of our website (user-interface web app): we exposed the participants to some tasks related to the website (our prototype) to complete, and then we asked for participants' satisfaction on the website.
3. IoT devices' usage: we asked the participants about the number of hours they use their IoT device per week, for what purposes they use them, what kind of information they think IoT devices can capture it, and whether they use any application to manage their IoT devices.
4. Participants' privacy attitudes: we asked the participants about their privacy views in general and related to IoT devices.
5. Participants' willingness to take actions in order to protect their personal information that is captured by IoT devices: we explored participants' views by exposing them to some scenarios and using 5-point Likert-scales from (1 = "Very Unimportant" to 5 = "Very Important"), and (1 = "Strongly Disagree" to 5 = "Strongly Agree").

4.5 Data Analysis and Results

In this section, we present an analysis of participants' responses to the survey addressing our hypotheses identified in Section 4.1.3.

We started the process of analysis by filtering the collected data and removing two incomplete surveys for the participants who did not agree to complete the survey. We analyzed responses from 43 participants between the ages 18 and 54. Participant demographics are summarized in Table 1.

4.5.1 Demographic Information

Out of 43 participants responded to the question of age, 6 were between the ages 18 and 24, 26 were between the ages of 25 and 34, 6 were between 35 and 44, and 5 were between 44 and 54 (Table 1). Most of the participants were in the 25-34 age range.

We asked the participants about their level of education. The result is available in Table 2. However, education is a core demographic question because participants in different levels of education may answer differently based on their background in technology and specifically in IoT devices.

According to our survey, many participants own more than one IoT device. The most chosen device was smartphones with a percentage of 90.70%, followed by

Smartwatch and smart TV with an equal percentage of 55.81%, then comes the rest of the devices with various percentages as seen in Table 1.

Table 1: Participants' Demographic Information

<i>Demographic</i>	<i>Number</i>	<i>Percent</i>
Age		
18-24	6	13.95%
25-34	26	60.47%
35-44	6	13.95%
45-54	5	11.63%
Education Background		
High school	6	13.95%
Bachelor's degree	21	48.84%
Master's degree	14	32.56%
Ph.D. or higher	2	4.65%
IoT Devices Owned by the Participant		
Smartphone	39	90.70%
Smartwatch	24	55.81%
Activity tracker	10	23.26%
Smart refrigerator	4	9.30%
Smart speaker (e.g., Amazon Echo, Google Alexa)	7	16.28%
Smart thermostat	3	6.98%
Smart TV	24	55.81%
None	1	2.33%

Additionally, we asked the participants how many hours per week they use IoT devices at different places such as home and workplace. The study indicates that around 42% of participants tend to use their IoT devices at home from 4 to 6 hours per week, whereas approximately 23% of participants tend to use their IoT devices at home from 7 to 10 hours per week. Moreover, around 44% of participants tend to use their IoT devices at work from 4 to 6 per week, and around the same percentage of participants tend to use their IoT devices at other places at the same rate of hours per week. Around 29% and 13% of participants tend to use their IoT devices from 7-10 hours per week at work and at other places, respectively (figure 8).

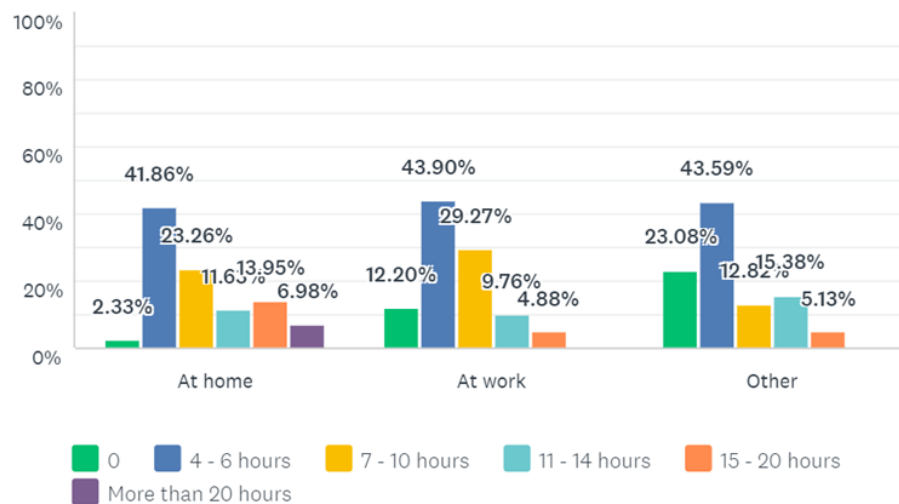


Figure 8 – Number of Hours Using IoT Devices

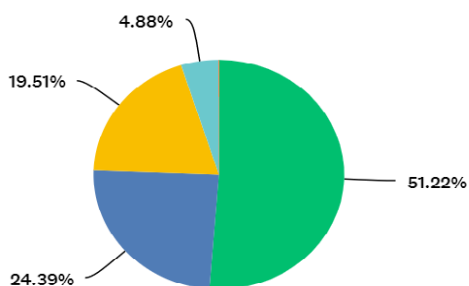
4.5.2 Primary Analysis

In this section, we analyzed the data of some questions of our survey that are related to the study hypotheses by representing the descriptive statistics, and the inferential statistics associated with the hypotheses.

4.5.2.1 Descriptive Statistics

Using 5-point Likert scales (1 = “Very Unimportant”, 5 = “Very Important”), the participants expressed their views about the importance of privacy and convenience when they are using smart devices. The results are available in Figure 9. Approximately half of the participants believed that privacy is very important when using smart devices, and less than a third of the participants believed that convenience is very important when using smart devices.

Privacy



Convenience

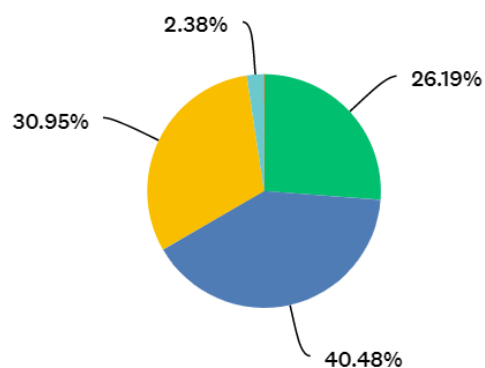


Figure 9 – Privacy and Convenience Importance

From the question of “how many hours per week do you use IoT devices”, we categorized the participants into three different groups according to their usage level of IoT devices: Low-frequency users (use IoT devices from 0 to 6 hours per week at home), Moderate users (use IoT devices from 7 to 14 hours per week at home), and Intensive users (use IoT devices from 15 to more than 20 hours per week at home).

Table 2: Categorizing the Participants Based on their Use of IoT devices

PARTICIPANTS' GROUPS	Low-Frequency Users		Moderate Users		Intensive Users		Total
	0 – 1 Hour	4 – 6 Hours	7 – 10 Hours	11 -14 Hours	15 – 20 Hours	More Than 20 Hours	
At Home	2.33%	41.86%	23.26 %	11.63%	13.95%	6.98%	100%
	1	18	10	5	6	3	43

We explored participants' views about the importance of some actions in terms of protecting their personal information that is captured by IoT devices, using 5-point Likert scales (1 = “Unimportant”, 5 = “Very Important”). The results are available in Figure 10. Around half of the participants thought that enabling them to control what information is being collected about them by IoT devices is very important, and more than a third of the participants found that this action is somewhat important. Moreover, more than a third of the participants believe that informing them when

their personal information is being collected by IoT devices is very important and may help in protecting their personal data, more than 40% of participants also believe that this action is important. More than 45% of participants believed that requesting their permission to collect their information by IoT devices before it is collected is very important, and 19% believed it is important. Note that the participants here were from all three groups divided according to the amount of their use of the IoT devices.

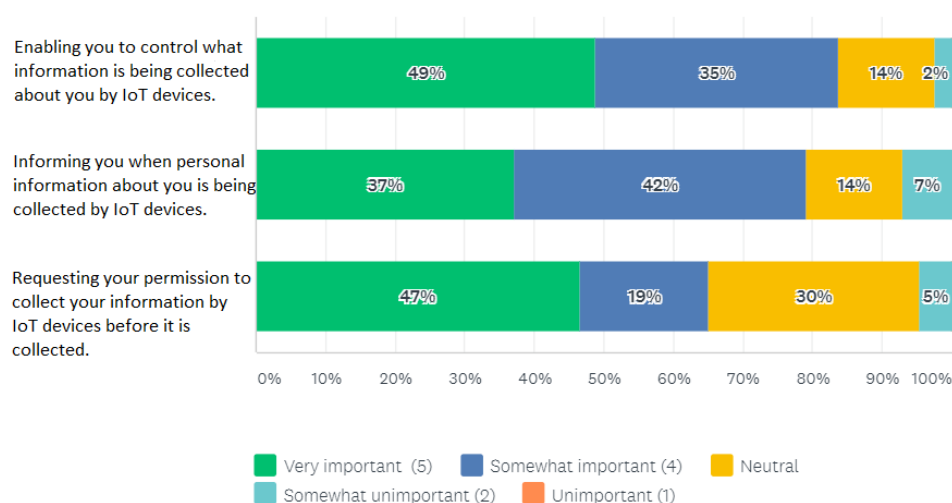
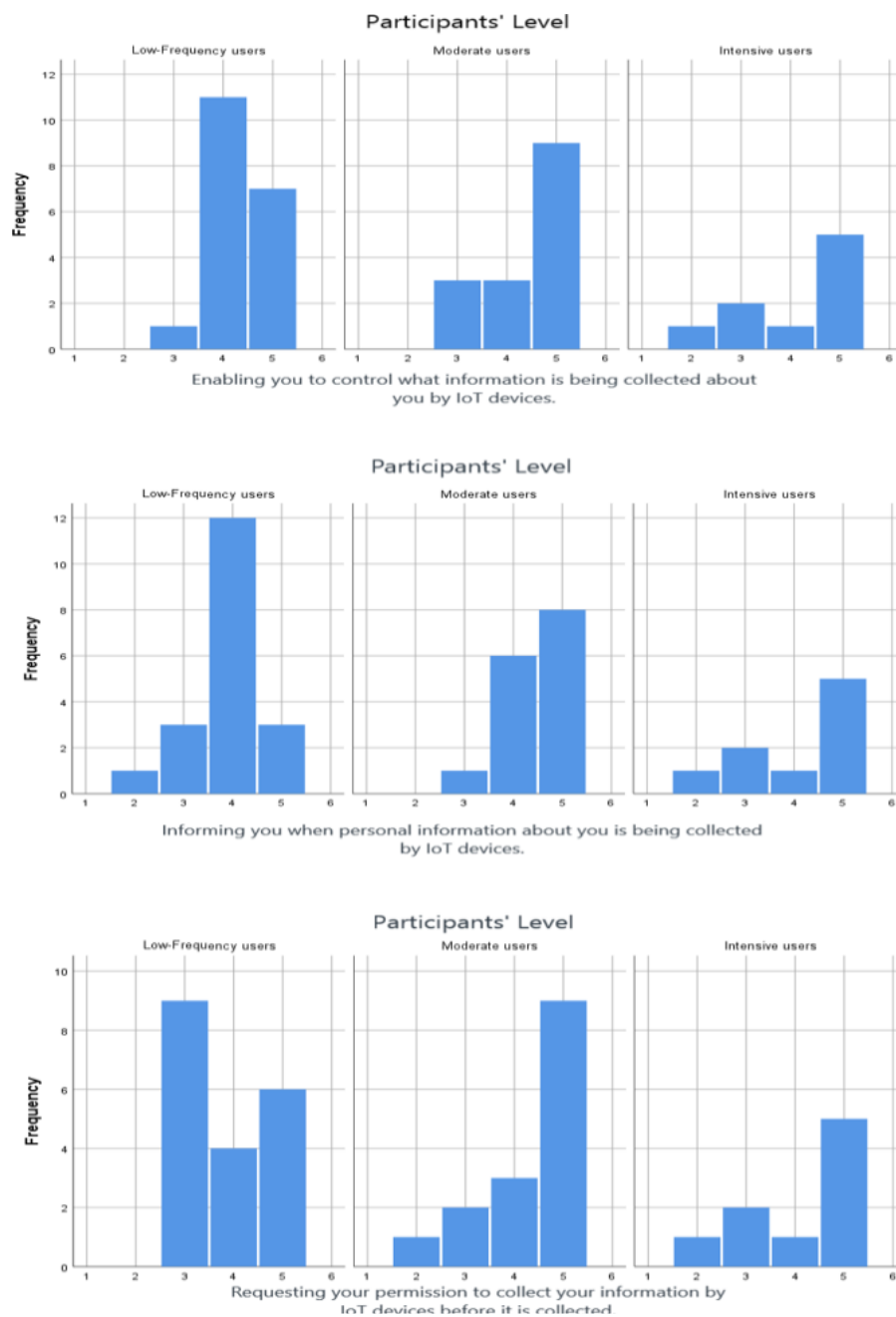


Figure 10 – Importance of Actions to Protect Personal Information

In the following figure, we used the identified groups of participants (low-frequency users, moderate users, and intensive users) with the same question above. The results showed that most of the participants, whether they use the devices very little, moderately or intensively, they consider all three actions very important or somewhat important to them in order to protect their personal information when they are using IoT devices.



(5) Very Important (4) Somewhat Important (3) Neutral (2) Somewhat Unimportant (1) Very Unimportant

Figure 11 – The Effect of the Amount of Use of IoT Devices by Users on the Importance of Some Actions to Protect Personal Information

Also, we explored the participants' satisfaction with our prototype of the website by asking them the following question: "Based on your experience in our website how satisfied are you with the website organization, ease of website navigation, and user-friendly interface." Using a 5-point Likert scale (from "1= Very Dissatisfied" to "5= Very Satisfied"), the average scores for the participants out of 5 were 4.07, 4.23, and 4.30 respectively (Figure 12).

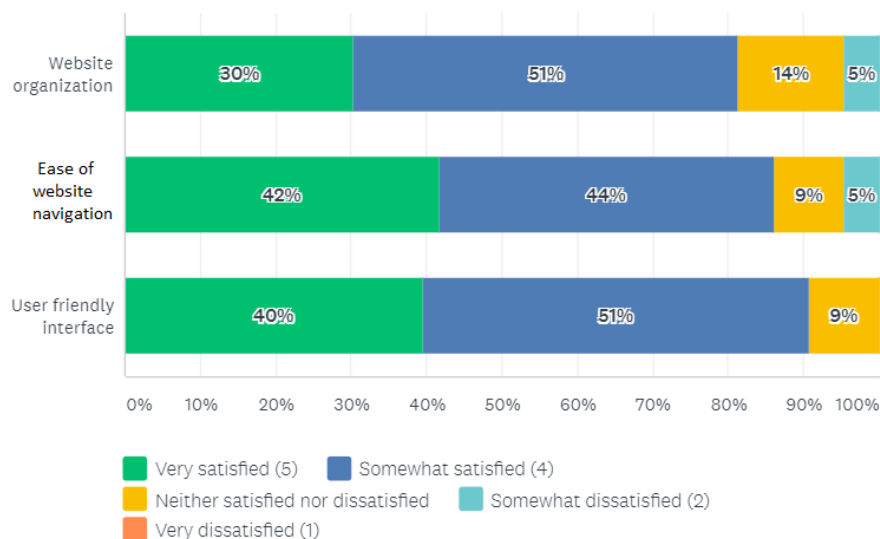


Figure 12 – Participants' Satisfaction of the Website

4.5.2.2 Inferential Statistics

All statistical analyses were computed using statistics software *IBM SPSS Statistics* and assumed a significance level of $p < 0.05$.

In order to examine our hypothesis *H1* hypothesized that when users use smart devices, privacy is more important to them than convenience. We conducted a dependent t-test for paired samples to compare the means of privacy and convenience to determine whether there is a statistically significant difference between them. We found that privacy ($M = 4.23$, $SD = .922$) and convenience ($M = 3.86$, $SD = .861$) were significantly different ($p = 0.010 < 0.05$), and the mean value of privacy is higher than the mean value of convenience.

Referring to *H2*, we have hypothesized there is no effect of the usage amount of IoT devices by users on the importance of the following actions to them to protect their personal information that is captured by IoT devices: being able to control what information is collected about them by IoT devices, being informed when their personal information is collected by IoT devices, and request their permission to collect their information by IoT devices before it is collected. We utilized our identified groups of the participants (low-frequency users, moderate users, and intensive users) in conducting a non-parametric test (Kruskal-Wallis test) to determine if there were statistically significant differences between the IoT usage amount (low-frequency users, moderate users, and intensive users) on the importance of those actions. We found non-significant results on the p -values ($p > 0.05$). Therefore, there is no statistically significant difference between the IoT usage levels for all actions, and all actions were important for most participants based on the mean

values. The results are available in Table 3, which shows the mean values, standard deviation, and p -values.

Table 3: P -value for Each Action

	Low-Frequency users	Moderate users	Intensive users	
Actions	Mean			p-value
<ul style="list-style-type: none"> Enabling you to control what information is being collected about you by IoT devices. 	4.32	4.40	4.11	0.777
<ul style="list-style-type: none"> Informing you when personal information about you is being collected by IoT devices 	3.89	4.47	4.11	0.98
<ul style="list-style-type: none"> Requesting your permission to collect your information by IoT devices before it is collected. 	3.84	4.33	4.11	0.279

In order to assess participants' satisfaction towards our prototype (website) three factors were generated; Web organization ($M = 4.12$, $SD = .731$), Ease of the website navigation ($M = 4.30$, $SD = .741$), and User interface ($M = 4.35$, $SD = .650$) on a 5-point Likert-scale (from "1 = very unsatisfied" to "5 = very satisfied"). With regard to $H3$, our hypothesis that the participants will be satisfied with the website organization, ease of website navigation, and the user-interface when they experience it was supported based on the participants' responses and the mean values of these factors.

4.5.3 Supplementary Analysis

In this section we presented the descriptive statistics of all remaining survey questions.

4.5.3.1 Participants' Understanding of the Website (User-Interface Web App)

The three tasks in the survey contained three different open-ended questions, which have two possibilities, wrong or correct answers; hence, we created tags for these questions, number one for the correct answer and zero for the wrong answer. These tags can allow us to determine the percentage of correct answers for each question.

3 of the participants skipped these tasks and we accept that because we allowed skipping questions for the participants' convenience. Therefore, 38 out of the 43 participants completed the tasks and answered the related questions. In the first task, participants were required to determine the number of currently connected devices on the website account, 35 out of 38 participants answered this question correctly (Figure 13).



Figure 13 – How Many IoT Devices are Currently Connected to this Website?

The second task contained some instructions for the participants, where they were asked to turn on the sensor readings function for the temperature and pressure sensor (IoT device), and then they were asked to determine the number of current readings available for the temperature and pressure sensor. Figure 14 shows that 36 out of 38 participants were able to follow the instructions and were able to use the web interface and answer the question correctly.



Figure 14 – How Many Temperature Readings are Currently Listed for the BMP180 Temperature and Pressure Sensor?

In the third task, participants were asked to determine the temperature readings for a specific date and time, and as can be seen in Figure 15, only one participant answered the question incorrectly.



Figure 15 – What was the Temperature Reading at 07:28:44 on 10/24/2019?

4.5.3.2 IoT Devices' Usage

Table 4 shows that many participants out of the 43 participants use IoT devices for different purposes, such as Smart Home products that usually help in saving time, cost, and energy. For example, people may like to switch off light remotely or after they left home and control their coffee machine from their Smart Phone to have a hot cup of coffee when they wake up. Our study indicates that around 40% of participants use their IoT devices for Smart Home purposes, and around 27% of participants use Vehicle tracking products that may be used for security purposes in case their vehicle gets stolen. While the most significant percentage is around 70% of participants use IoT devices for entertainment purposes, which include several IoT devices such as Smart TV, virtual games, Smart toys, and Smart Wristband. Lifestyle is also one of the most common purposes that people use IoT devices to improve their lives. For example, in sport, people can use wearable devices for their performance efficiency. Our study shows that more than 60% of participants tend to use their IoT devices for lifestyle.

Moreover, for health monitoring, people can use Smart tracking devices to track their sleeping pattern and check-up schedule. Thus, as can be seen in our study, around 42% of participants use IoT devices for health monitoring. However, less than 5% of participants had no IoT devices at all.

Whereas the participants were asked whether they are using one of the listed applications for IoT management such as Wink, SimpliSafe Home Security, Yonomi, ADT control, and Olisto. The study shows that 60% of the participants do not use any of the typical IoT manager applications and similar low ratios to the rest of the other applications of IoT management, results are available in Table 4.

Table 4: IoT Devices' Usage

IoT Devices' usage	Number	Percent
Purposes		
Smart Home	18	41.86%
Vehicle Tracking	12	27.91%
Entertainment	30	69.77%
Lifestyle	26	60.47%
Health monitoring	18	41.86%
None (do not have an IoT device)	2	4.65%
IoT management Application		
Wink		
SimpliSafe Home Security	4	9.30%
Yonomi	4	9.30%
ADT Control	0	0.00%
Olisto	4	9.30%
None	1	2.33%
Do not have an IoT device	26	60.47%
	4	9.30%

To discover how the participants understand IoT devices, we inquired about the type of information that they believed would be captured by specific IoT devices, such as Smart Thermostat, Smart Tv, and smartphone, if they were using it. Figure 16 represents participants' choices for different types of data that they expect to be sensed when using the previous devices.

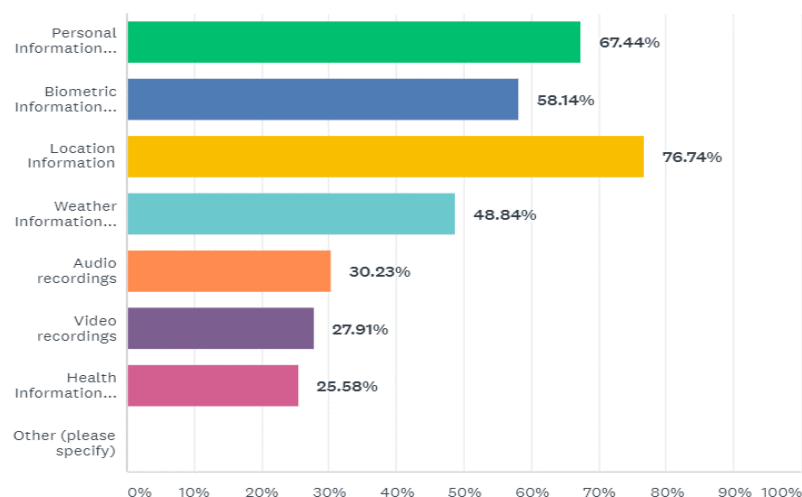


Figure 16 – Data Captured by Specific IoT Devices

4.5.3.3 Participants' Privacy Attitudes

We also asked the participants how concerned they are about privacy in their daily life to evaluate the participants' privacy perception in general. Using 4-point Likert-scale (1 = "Not at all", 4 = "Very Concerned"), participants express their

views (see Table 5). Thereby, we indicated from the mean and standard deviation values ($M > 2.5$) that most participants are somewhat concerned about their privacy in general.

Table 5: Privacy in Daily Life (1 = “Not at all”, 4 = “Very Concerned”)

Statements	Mean	Standard Deviation
People knowing your private and personal information	2.98	1.00
Walking in a public place which is full of sensors such as, private security Camera, traffic microwave radar sensor.	2.30	0.98
To be in the background of photos that are taken by strangers	2.65	0.99
To be in the foreground of photos that are taken by strangers	2.86	1.02

We explored participants’ perceptions of ranking the responsible authority, from the governments, IoT devices’ manufacturers, or IoT users, in users’ privacy protection when using IoT devices. Figure 17 shows the numbers of participants who ranked the responsible authority regarding protecting IoT users’ privacy, in terms of its importance to them from 1 to 3, where one is most important to them, and three is least important to them.

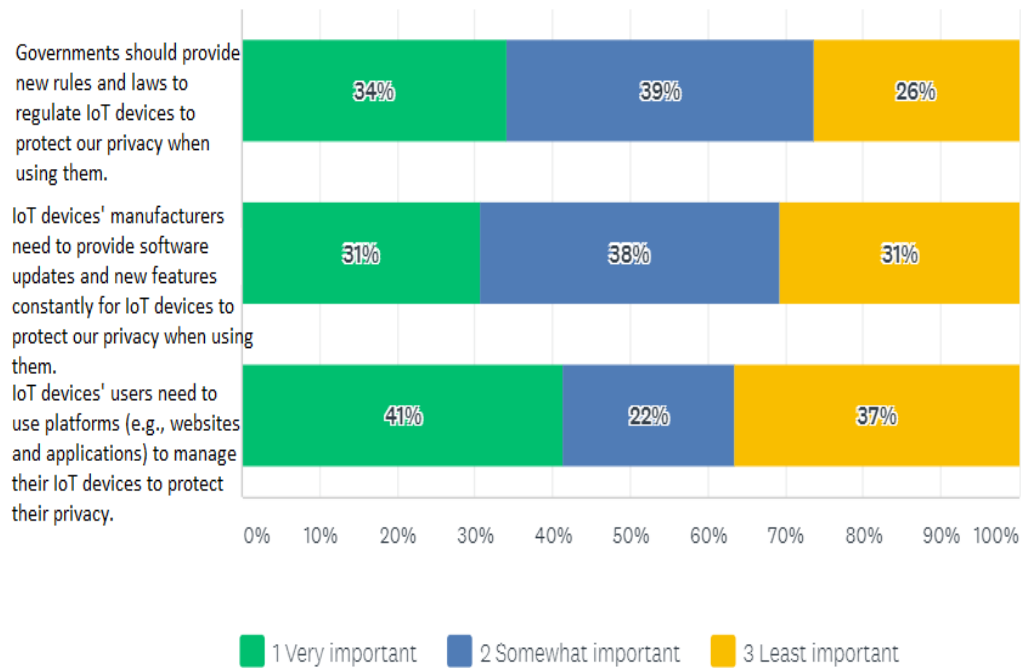


Figure 17 – Statements Rank

4.5.3.4 Participants' Willingness to Take Actions in order to Protect their Personal Information that is Captured by IoT Devices

Using 5-point Likert scale (1 = “Strongly Disagree” 5 = “Strongly Agree”), participants expressed their views about different aspects regarding managing IoT devices and reducing the risk of privacy breaching, when they assumed that they live in a Smart home that contains different IoT devices and sensors which are: Smart Tv, Smart light, Smart Thermostat, and Smartwatch) that capture various types of their information (e.g., their personal information, room temperature degree, their heart

rate, their TV watching preferences). Figures 18, 19, and 20 below summarize participants' opinions about the following actions: "I am concerned about the privacy of data sensed about me when using IoT devices", "I prefer to use ONE platform (e.g., website) to manage all my IoT devices", and "I prefer to use website to manage my IoT devices rather than a particular application". Figure 18 shows us that the majority of the participants (= 79%) are concerned about the privacy of their data sensed when they are using IoT devices.

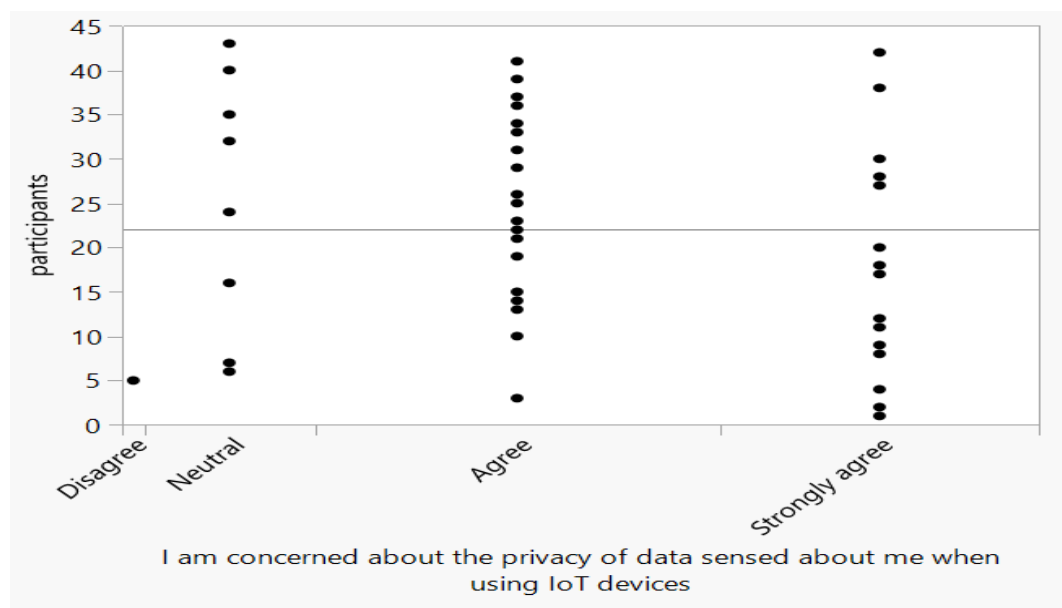


Figure 18 – Participants' Responses (Privacy Concerns)

Also, the majority of the participants (= 74%) prefer to use a website to manage their IoT devices rather than a particular application, as shown in Figure 19.

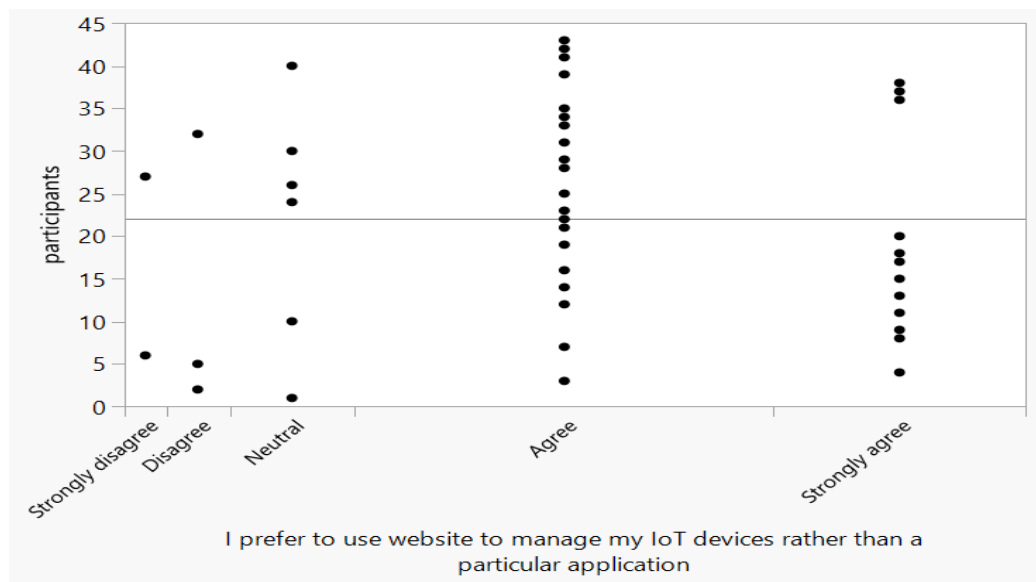


Figure 19 – Participants' Responses (Using Website for IoT Management)

Furthermore, a significant number of the participants (about 70%) prefer to use one platform to manage all of their IoT devices and reduce the risk of privacy breaching when they live in a Smart home that contains different IoT devices, and sensors Figure 20.

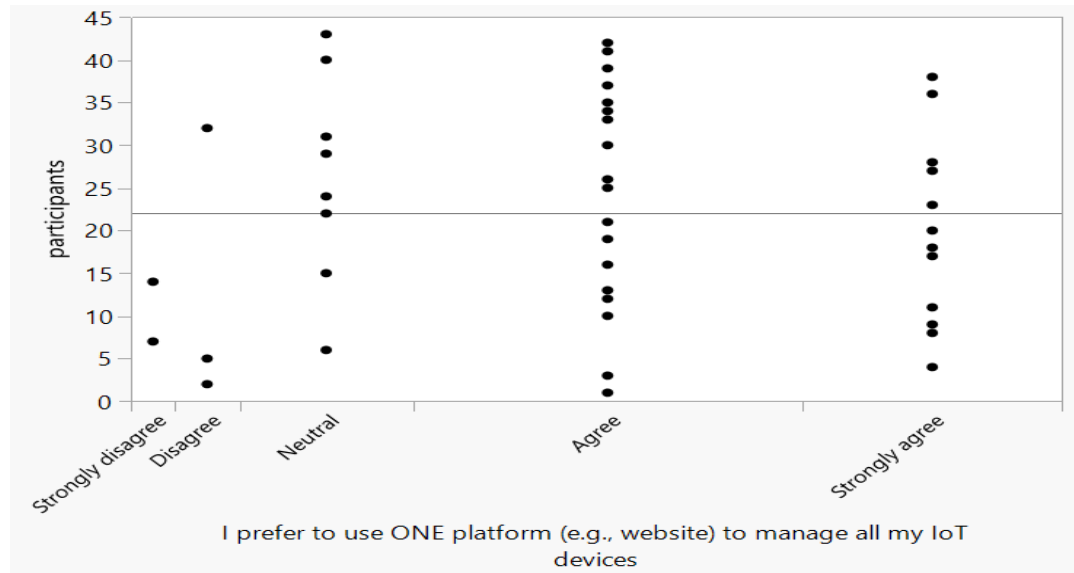


Figure 20 – Participants’ Responses (Use One Platform for All IoT Devices)

Using another 5-point Likert scales (1 = “Unimportant” 5 = “Very Important”), participants expressed their willingness to take actions to protect their privacy when they are at a friend’s house, and they have a security camera which is recording audio and video that is kept for one week (Hypothetical Scenario). The results are available in Figure 21. Most of the participants were willing to take specific actions to protect their personal information that is captured by that IoT device.

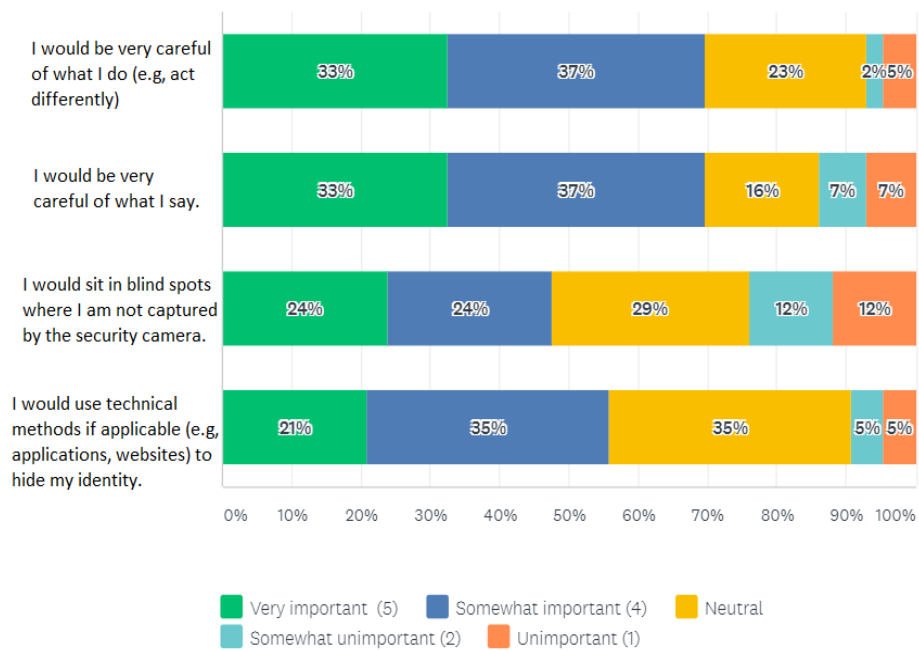


Figure 21 – Hypothetical Scenario Responses

4.6 Discussion

Some of the previous works have further investigated the factors that may affect people's opinions about IoT adoption. According to [105, 106], privacy issues were the reason behind the abandonment of technology from users. According to a new smart device [survey by Consumers International and the Internet Society](#) [107], 75% of people do not trust the way of sharing data by connected devices.

In the same direction, we investigated our participants' views on the importance of privacy and convenience when using smart devices. Our findings from the *H1* hypothesis test shows that privacy is more important than convenience for the participants when they are using smart devices, and these participants are part from IoT users around the world who may avoid using IoT devices due to the compromise of user privacy in the way of collecting data. Therefore, preserving user privacy is crucial in the IoT environment, which can be done via our proposed solution (the website).

However, people still buy these devices that can access their lives and capture their information. Around 70% of the participants of [survey by Consumers International and the Internet Society](#) [107], said they own one or more connected devices, that include smart home appliances, fitness monitors, and gaming consoles. Moreover, according to marketing research firm IDC, last year, the sales of smart devices increased 25 percent [108]. Accordingly, we were interested in whether the participants' levels in the use of IoT devices affects the importance of some actions such as, allowing users to control what information is collected about them by IoT devices, informing users when their personal information is collected by IoT devices, and requesting users' permission to collect their information by IoT devices before it is collected, in order for those users to protect their personal information that can be captured by IoT devices. By comparing our groups, low-frequency users, moderate users, and intensive users, from our *H2* hypothesis test, we found that there

is no relationship between the participants' level in using IoT devices and their attitudes with the actions in order to protect their privacy. This means the intensive use of smart devices by users does not affect their perceptions of using IoT devices and this might suggest they do not have significantly more knowledge about IoT devices and how these devices work. Therefore, intensive users of IoT devices are might not experts in IoT who supposed to be able to protect their privacy; thus, they still need a tool that can help them to protect their personal information and their privacy when using IoT devices which can be achieved by using the proposed website. Furthermore, we introduced our participants to some tasks to do on the website (prototype) and experience our prototype. Our findings from the *H3* hypothesis test confirmed that most participants were satisfied with our prototype (website). Thus, we can optimize the website in the future in the same way as the current design of the website.

On the other hand, experts have explained why people still buy these devices even when they do not trust them; people may not understand the extent of data collected by smart devices, people may think of the trade-off is worth it, there are no more options for consumers, people suppose the government will take care of it, and some people do not care enough about privacy to take action about it [109]. Besides, eleven semi-structured interviews were conducted with owners of Smart Home to discover their reasons behind the purchasing of IoT devices, beliefs of smart home privacy risk, and how they protect their privacy from external entities [110]. The

recurring themes from the study show that users value convenience and connectedness that can affect their privacy opinions, the perceived benefit from the external entities affects users' opinions about who should access to their smart home, and users trust the IoT device manufacturers in protecting their privacy without any awareness of the machine learning potential to reveal sensitive information from non-audio/visual data [110]. Even though IoT may improve the convenience of users' lives, and most people may prefer convenience over potential risk, it invades our privacy as well. Returning to figure 16, we found that the participants' choices of the data types that they believed would be captured by specific IoT devices, such as Smart Thermostat, Smart TV, and smartphone were not accurate. Therefore, we can infer that most of the participants do not understand IoT devices and what type of data can be sensed about them by a particular device, which confirmed that IoT users' lack of awareness about IoT devices and their need to be more knowledgeable and aware about IoT devices in order to protect their privacy. These findings provide evidence of unawareness of some users about privacy risks related to using Internet-connected devices, including IoT devices, and suggest the need to provide a new concept that can protect users' privacy without changing their opinions about the convenience goal of using IoT devices.

Our findings supported the previous work , that people may care more for their privacy when using smart devices, in addition to that some of them may avoid

using smart devices due to the privacy issues related to Internet-connected devices. Further, in the case of people who would value convenience over privacy in using smart devices, this is due to many different factors that can affect their opinion including their lack of awareness of smart devices, which our findings supported the previous work in this aspect as well.

Referring to the supplementary analyses of our survey, we found that the completion of the defined tasks in the beginning of our survey by the participants indicates that the proposed prototype is an easily accessible platform, and it can be used easily by the participants with different levels of education and different levels in using IoT devices without much technical experience. This supports our mentioned aim, which was providing an easy to use platform for IoT users. Moreover, based on this study, there is a widespread use of IoT devices, and most of the participants are familiar with IoT devices. Besides, table 4 shows that the participants tend to use their IoT devices for different purposes, so that we inferred that the majority of the participants own IoT devices and use them consistently during the week for many purposes. Also, table 4 represents that 60% of the participants do not use any of the typical IoT manager applications, which indicates the need for creating a single website platform where users can access it from various locations at any time for IoT devices management. Therefore, provide the IoT users with a web-based user interface may enable them to gather and connect all of their IoT devices to one platform and control them easily from any place such as home,

workplace, and vehicle through that platform. All these may contribute to improving IoT users' perception of their privacy when using IoT devices. Also, the website in the future needs to be compatible with many applications (categories) of IoT, that combines many devices. This feature will enable IoT users to be able to connect all of the IoT devices that are used by them for various purposes to the website easily.

According to figure 17, more than 40% of participants ranked the statement "IoT devices' users need to use platforms (e.g., websites and applications) to manage their IoT devices to protect their privacy" as number 1, which means very important to them. Therefore, we can infer that these participants believed that IoT users are responsible for protecting their privacy. Thereby, we need to facilitate the way of protecting their privacy when using IoT devices by providing them with our web-app user-interface.

Referring to our findings in section 4.5.3.4, we conclude that there is a crucial need for our solution in protecting users' privacy because the majority of our participants were concerned about their privacy about their data that sensed when using IoT devices. Moreover, a significant number of our participants prefer to use a website to manage their IoT devices rather than a particular application, and this confirms the need for our solution, which is a website that enables IoT users to manage their devices. Most of the participants as well prefer to use one platform to manage all of their devices, which confirms the importance of our platform that aims at enabling IoT users to gather all of their devices in one platform to facilitate the

managing process of these devices. Correspondingly, most of the participants were willing to take action in order to protect their personal information from exposure in the IoT environment. This can lead to the participants' desire to protect their privacy, which can be achieved by using our proposed solution by enabling them to manage their IoT devices in order to protect their privacy.

However, protecting users' privacy when they use IoT devices means managing these devices. Thus, some users use physical devices to manage some of their IoT devices, such as smart home speakers. Eventually, many smart home speakers used to manage devices and services, such as Amazon Echo smart speakers or Google Home devices. They have Google Assistant built-in so that they can achieve the same tasks, such as controlling the light and changing the thermostat. However, these speakers are varied in designs and specifications based on the locations and purposes of use.

Specifically, Google Home Hub made by Google with a display touchscreen (7 inches); it has Google Assistant built into it. Google Home Hub has a mute switch so that the user can mute Google Assistant. Google Home Hub has two far-field microphones to allow it to hear the user when activating it with the activate commands, and it has an EQ ambient sensor to adjust the display based on the lighting automatically. Google Home Hub can be activated by voice and do any tasks of Google assistant, and it does not have apps that users can download, however, all it can do is stream from the Internet instead. There is no web browser on Google

Home Hub that allows the user to ask it to pull up specific Google search images, for instance. Google Home Hub enables users to stream media and music from, and it is a cast device so anything that users have on their phone it can cast, for example, ask it to play some news and it will pull up the latest news report in a video form so that users can watch it. The most functions that can be achieved by the Google Home Hub are controlling the light, cast media, broadcast, and message, change the thermostat, view smart camera, and change the TV supported devices [111].

Even though the Smart Home speakers including Google Home are used to manage devices and services, it could also have the reverse effect, because they are considered as IoT device that can collect personal information about users, and this information may be retained, used, or sold without the users' permission.

Therefore, our proposed paradigm (web app) is intended to dispense with hubs, and it focuses on privacy-preserving to contribute to changing users' perception of privacy when using IoT devices. This web app does not require a specific operating system, and it is designed to do multiple functions such as controlling, monitoring, and managing devices. It also intended to be compatible with various brands and devices in many IoT applications that are widely used. The web app will enable users to connect their IoT devices to it, and then they can view details of the devices and check their status. The web app provides some features like the ability to monitor devices' connections quality, control devices remotely such as creating smart rules (operations), manage device software, view operations of the

device such as pending, and execution in real-time, and manage device permissions for a device, for example, change devices' passwords. Moreover, the web app focuses on using real-time monitoring in order to make an instant decision to events from sensors, derive data according to specific rules, and automated control actions remotely by automated trigger based on events.

4.7 Study Limitations

This section outlines some of the study limitations that might have affected our results.

1. The study was biased by the fact that 60% of the participants were between 25 and 34 years old. Also, 86% of our participants had at least a bachelor's degree. We may have some difficulties in generalizing the result because the general population is not necessarily at this age and does not have the same education level. As a result, the number of participants conducting the survey cannot be entirely representative of the desired population.
2. More than half of the participants do not use any applications for IoT devices management, this could affect their opinion as it is their first time to experience such a platform, so they do not have any background of other platforms in the same direction. Hence, this information should be considered when reviewing their answers relating a comparison to other platforms.

3. In our study, the participants were asked to imagine themselves into hypothetical situations that are limited in what they can cover, and we found that privacy is more important to them than convenience when using smart devices, and most of the participants were unusually privacy-sensitive. Therefore, our study may be susceptible to this bias because the scenarios were abstract, and participants were asked to imagine themselves in situations they may not have encountered.
4. The small number of participants. As a result, we did not have sufficient data to be able to generalize the findings to the entire desired population.
5. In our study, designing and implementing the proposed website would be a challenging task due to some of the reasons mentioned above in the website chapter. Thus, this study only developed an experimental prototype to validate the proposed framework. The prototype we provided covered the main idea of IoT website management, and it did not cover some potential concerns that might face IoT users when using the website, such as security challenges.

4.8 Summary

This chapter explained the study design that we employed to test our study's hypotheses, and it described the participants, the instruments used, the procedure of data collection, and the statistical tests that have been used for data analysis and

interpretation. By conducting this study, we were able to gather valuable information that led to addressing our hypotheses. Finally, this chapter outlined the study limitations.

Chapter 5

Conclusion and Future Work

Due to the advances in IoT technology and the increasing number of IoT devices, several concerns are arising regarding the privacy perspective of using such devices. This research aimed at providing an effective platform for IoT users that can facilitate controlling and managing their IoT devices remotely with real-time data monitoring in order to protect their privacy. In this research, we have proposed a web-based user interface which had specific functionalities that could be seen in; controlling an IoT device remotely, accessing information about an IoT device, controlling what information can be collected from an IoT device, and setting some privacy preferences for a specific IoT device. The advantages of this web app are that it could be accessed via different operating systems and it does not require any advanced technical skills. However, the descriptions mentioned above were not all had been implemented since there was a need to integrate APIs for IoT devices to connect them directly to the web app. Whereas, each device has a distinct set of capabilities, protocols, commands, and functionalities. Therefore, there was a need to integrate a related API for each device. Thus, a prototype was created to which it can be used to demonstrate the concept of the proposed web-app. A survey was conducted to

examine the implementation of the prototype and its effects on the IoT users' perceptions about privacy in the IoT environment. The findings confirmed the need for creating a platform where users can control various IoT devices remotely. It also indicated that the website is a user-friendly platform, and it could be used easily without any technical experience. Users were able to access information about the connected IoT device as well as switch on/off the device.

5.1 Research questions and Research Hypotheses

This research was driven by a research questions and related hypotheses. The research questions are:

Q 1- When using smart devices, is privacy or convenience more important for users?

Q 2- Does the amount usage of IoT devices by users have an effect on the importance of the following actions to them: “allowing users to control what information is collected about them, informing users when their information is collected, and requesting users' permission to collect their information”, to protect their personal information that is captured by IoT devices?

Q 3- To what extent does offering an independent web interface, which does not require a specific operating system or separate software development for IoT devices management, gain users' satisfaction?

The hypotheses that were derived from the above research questions and how

they were addressed are as follows:

H1: When users use smart devices, privacy is more important to them than convenience.

This hypothesis is supported. This decision is based on our findings of comparing the means of privacy and convenience to determine whether there is a statistically significant difference between them. We found that privacy ($M = 4.23$, $SD = .922$) and convenience ($M = 3.86$, $SD = .861$) were significantly different ($p = 0.010 < 0.05$), and the mean value of privacy is higher than the mean value of convenience.

H2: The amount usage of IoT devices by users does not affect the importance of the following actions to them: allowing users to control what information is collected about them, informing them when their personal information is collected, and requesting their permission to collect their information before it is collected, in terms of protecting their information that is captured by IoT devices.

This hypothesis is supported. This decision is based on the result of our statistical test which shows that there is no significant effect of participants' level in using IoT devices when they want to protect their personal information so that there is a need to offer a web app that helps in protect their information by enabling them to manage the collected information about them by their IoT devices.

H3: When the participants experience the web-user interface (The prototype for our website), they will be satisfied with the website organization, ease of website navigation, and the user interface.

This hypothesis is supported. This decision is based on the participants' responses analysis and the mean values of the defined factors of the website (website organization, ease of web navigation, and user interface). Most of our participants were satisfied with the website organization ($M = 4.12$, $SD = .731$), ease of web navigation ($M = 4.30$, $SD = .741$), and user interface ($M = 4.35$, $SD = .650$).

Finally, to answer the research questions: first, based on the findings of this study we found that the privacy is more important for the users than convenience when using smart devices, therefore, they need to have a way to protect their privacy when using smart devices including IoT devices. Second, the participants' level in using IoT devices has no effect on the importance of the following actions to them: "allowing users to control what information is collected about them, informing users when their information is collected, and requesting users' permission to collect their information", to protect their personal information that is captured by IoT devices. Thus, by providing IoT users who are in different levels in using IoT devices with a solution which can offer the same measures to them in order to protect their privacy, they will be willing to use it. Third, most the participants were satisfied with the website in terms of its organization, ease of the navigation, and the user interface, hereby, we can optimize our prototype with the same design and offer it to IoT users to enable them to manage their IoT devices from one platform and preserve their privacy.

5.2 Future Work

The work presented here is just a prototype to prove the concept of the website implementation for IoT devices management. We plan to widen the validation of the proposed platform by taking into account the APIs integrations for IoT devices that allow them to be controlled from the website. Our prototype needs some other work to be done in the near future, such as adding more features, more common user interface features to improve users' experience. Besides, the security system may be added to provide more features, more IoT categories and devices may be added as well in parallel with the functions to enhance the website functionalities. Moreover, in the future, this platform can be modified, providing extra features such as voice control.

References

- [1] “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016,” *Gartner*. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>.
- [2] A. Perez, S. Zeadally and S. Griffith, "Bystanders' Privacy", *IT Professional*, vol. 19, no. 3, pp. 61-65, 2017. Available: 10.1109/mitp.2017.42.
- [3] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, & N. M. Sadeh, “Privacy Expectations and Preferences in an IoT World” . *SOUPS*. 2017.
- [4] k.Ashton, Rfidjournal.com,2009. [Online]. Available: <https://www.rfidjournal.com/articles/pdf?4986>.
- [5] L. Srivastava, and I. T. Union, “ITU Internet Reports: The Internet of Things”, 2005.
- [6] “Internet of Things (IoT) History,” Postscapes. [Online]. Available: <https://www.postscapes.com/internet-of-things-history/>.

- [7] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, and European Commission. Directorate-General for the Information Society and Media, “Vision and Challenges for Realising the Internet of Things”, 2010.
- [8] Y. Huang and G. Li, “A Semantic Analysis for Internet of Things,” 2010 International Conference on Intelligent Computation Technology and Automation, 2010.
- [9] L. Coetzee, and J. Eksteen, “The Internet of Things - promise for the future? An introduction”, 2011. Retrieved from https://ieeexploreieee_org.portal.lib.fit.edu/stamp/stamp.jsp?tp=&arnumber=6107386
- [10] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
- [11] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
- [12] J. Ibarra-Esquer, F. González-Navarro, B. Flores-Rios, L. Burtseva, and M. Astorga-Vargas, “Tracking the Evolution of the Internet of Things Concept Across Different Application Domains,” Sensors, vol. 17, no. 6, p. 1379, 2017.
- [13] A. S. Reddy, “Reaping the Benefits of the Internet of Things.”

- [14] A. Gupta, P. Gupta, and J. Chhabra, "IoT based power efficient system design using automation for classrooms," 2015 Third International Conference on Image Information Processing (ICIIP), 2015.
- [15] M. Elkhodr, S. Shahrestani and H. Cheung, "The Internet of Things: Vision & challenges", IEEE 2013 Tencon - Spring, 2013. Available: 10.1109/tenconspring.2013.6584443.
- [16] Q. F. Hassan, A. ur R. Khan, and S. A. Madani, Internet of things: challenges, advances, and applications. Boca Raton: Taylor & Francis, CRC Press, 2017.
- [17] H.-D. Ma, "Internet of Things: Objectives and Scientific Challenges," Journal of Computer Science and Technology, vol. 26, no. 6, pp. 919–924, 2011.
- [18] S. Hsu, "IoT Security Guidelines Device Life Cycle Overview", 2019. Retrieved from <https://www.trendmicro.com/us/iotsecurity/content/main/document/IoT%20Security%20Whitepaper.pdf>
- [19] D. Serpanos and M. Wolf, "IoT System Architectures," Internet-of-Things (IoT) Systems, pp. 7–15, 2017.

- [20] V. Aleksandrovičs, E. Filičevs and J. Kampars, "Internet of Things: Structure, Features and Management", *Information Technology and Management Science*, vol. 19, no. 1, 2016. Available: 10.1515/itms-2016-0015.
- [21] H. Ning, "Unit and Ubiquitous Internet of Things," 2016.
- [22] Z. H. Ali, H. A. Ali, and M. M. Badaway, "Internet of Things (IoT): Definitions, Challenges and Recent Research Directions," *International Journal of Computer Applications*, vol. 128, no. 1, pp. 37–47, 2015.
- [23] A. Khalid, "International Journal of Advanced Computer Science and Information Technology," 2016.
- [24] J. Sathish kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20–26, 2014.
- [25] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 2012 10th International Conference on Frontiers of Information Technology, 2012.
- [26] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016.

- [27] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization", *Wireless Personal Communications*, vol. 58, no. 1, pp. 49-69, 2011. Available: 10.1007/s11277-011-0288-5
- [28] C. Sun, "Application of RFID Technology for Logistics on Internet
- [29] M. Matin and M. Islam, "Overview of Wireless Sensor Network," *Wireless Sensor Networks - Technology and Protocols*, Jun. 2012.
- [30] A. Botta, W. de Donato, V. Persico and A. Pescape, "On the Integration of Cloud Computing and Internet of Things", 2014 International Conference on Future Internet of Things and Cloud, 2014. Available: 10.1109/ficloud.2014.14.
- [31] N. Maor, "The Internet of Things (IoT) and your Wi-Fi needs", 2018. Retrieved from <https://www.celeno.com/blog/the-internet-of-things-iot-and-your-wi-fi-needs>
- [32] C. Davis, "Zigbee Alliance Accelerates IoT Unification with 20 Zigbee 3.0 Platform Certifications", 2016. Retrieved from <https://www.zigbee.org/zigbee-alliance-accelerates-iot-unification-with-20-zigbee-3-0-platform-certifications/>
- [33] T. Guarda, M. Leon, M. Augusto, L. Haz, M. Cruz, W. Orozco, and J. Alvarez, "Internet of Things Challenges".

- [34] S. Jafari, F. Mtenzi, R. Fitzpatrick, and B. O'Shea, "Security Metrics for e-Healthcare Information Systems: A Domain Specific Metrics Approach," *International Journal for Digital Society*, vol. 1, no. 4, pp. 238–245, Jan. 2010.
- [35] H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in eHealth", *Proceedings of the 7th International Conference on Body Area Networks*, 2012. Available: 10.4108/icst.bodynets.2012.250235.
- [36] S. Weiß, O. Weissmann, and F. Dressler, "A comprehensive and Comparative Matrix for Information Security", 2005.
- [37] H. Abie, "Adaptive security and trust management for autonomic message-oriented middleware", *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, 2009. Available: 10.1109/mobhoc.2009.5336915.
- [38] R. Savola, H. Abie, and M. Sihvonen, "Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications," *Proceedings of the 7th International Conference on Body Area Networks*, 2012.
- [39] N. Dulay, E. Lupu, M. Sloman, J. Sventek, N. Badr and S. Heeps, "Self-managed Cells for Ubiquitous Systems", *Lecture Notes in Computer Science*, pp. 1-6, 2005. Available: 10.1007/11560326_1.

- [40] Z. Li, X. Yin, Z. Geng, H. Zhang, P. Li, Y. Sun, H. Zhang, and L. Li, "Research on PKI-like Protocol for the Internet of Things," 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, 2013.
- [41] H. Ning, H. Liu, and L. T. Yang, "Cyberentity Security in the Internet of Things," Computer, vol. 46, no. 4, pp. 46–53, 2013.
- [42] A. Dohr, R. Modre-Opsrian, M. Drobits, D. Hayn and G. Schreier, "The Internet of Things for Ambient Assisted Living", 2010 Seventh International Conference on Information Technology: New Generations, 2010. Available: 10.1109/itng.2010.104.
- [43] L. You-Guo and J. Ming-Fu, "The Reinforcement of Communication Security of the Internet of Things in the Field of Intelligent Home through the Use of Middleware," 2011 Fourth International Symposium on Knowledge Acquisition and Modeling, 2011.
- [44] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and Access Control in the Internet of Things," 2012 32nd International Conference on Distributed Computing Systems Workshops, 2012.
- [45] M. Zhao, J. Walker, and C.-C. Wang, "Security challenges for the intelligent transportation system," Proceedings of the First International Conference on Security of Internet of Things - SecurIT 12, 2012.

- [46] S. Horrow and A. Sardana, "Identity management framework for cloud-based internet of things", Proceedings of the First International Conference on Security of Internet of Things - SecurIT '12, 2012. Available: 10.1145/2490428.2490456.
- [47] R. Aggarwal and M. Das, "RFID security in the context of "internet of things"", Proceedings of the First International Conference on Security of Internet of Things - SecurIT '12, 2012. Available: 10.1145/490428.2490435.
- [48] S. Sahmim and H. Gharsellaoui, "Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review," *Procedia Computer Science*, vol. 112, pp. 1516–1522, 2017.
- [49] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, Oct. 2013.
- [50] van Deursen T. 50 Ways to Break RFID Privacy. Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, vol. 352. Springer Boston, 2011; 192–205, doi:10.1007/978-3-642-20769-3 16.

- [51] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017.
- [52] *Security Guidance for Early Adopters of the Internet of Things*. 2015.
- [53] Sathish Kumar J, Patel DR (2014) A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications* 90.11
- [54] Kozlov D, Veijalainen J, Ali Y (2012) Security and privacy threats in IoT architectures. In: *Proceedings of the 7th International Conference on Body Area Networks (BodyNets '12)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, 256–262
- [55] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
- [56] X. Huang, R. Fu, B. Chen, T. Zhang, A. Roscoe, User interactive internet of things privacy preserved access control, in: *7th International Conference for Internet Technology and Secured Transactions, ICITST 2012*, London, United Kingdom, 2012, pp. 597–602.

- [57] J. Yang, B. Fang, Security model and key technologies for the internet of things, J. China Universities Posts Telecommun. 8 (2) (2011) 109–112.
- [58] Y. Wang, Q. Wen, A privacy enhanced dns scheme for the internet of things, in: IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.
- [59] A. Ukil, S. Bandyopadhyay, A. Pal, Iot-privacy: To be private or not to be private, in: Proceedings – IEEE INFOCOM, Toronto, ON, 2014, pp. 123–124.
- [60] J. Du, C. Jiang, E. Gelenbe, L. Xu, J. Li and Y. Ren, "Distributed Data Privacy Preservation in IoT Applications", *IEEE Wireless Communications*, vol. 25, no. 6, pp. 68-76, 2018. Available: 10.1109/mwc.2017.1800094.
- [61] L. Hu, Y. Qian, M. Chen, M. Hossain and G. Muhammad, "Proactive Cache-Based Location Privacy Preserving for Vehicle Networks", *IEEE Wireless Communications*, vol. 25, no. 6, pp. 77-83, 2018. Available: 10.1109/mwc.2017.1800127.
- [62] M. Seliem, K. Elgazzar, and K. Khalil, "Towards Privacy Preserving IoT Environments: A Survey," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–15, 2018.
- [63] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of things," 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016.

- [64] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 357430, 2014.
- [65] I. Bouij - Pasquier, A. Ait Ouahman, A. Abou El Kalam and M. Ouabiba de Montfort, "SmartOrBAC security and privacy in the Internet of Things", 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), 2015. Available: 10.1109/aiccsa.2015.7507098.
- [66] W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
- [67] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," *UbiComp 2002: Ubiquitous Computing Lecture Notes in Computer Science*, pp. 237–245, 2002.
- [68] S. A. Bagüés, A. Zeidler, C. F. Valdivielso, and I. R. Matias, "Sentry@ Home-Leveraging the smart home for privacy in pervasive computing", 2007.
- [69] T. Shinzaki, I. Morikawa, Y. Yamaoka, and Y. Sakemi, "IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data", 2016.

- [70] Z. Peterson, R. Burns, J. Herring, A. Stubblefield, and A. Rubin, "Secure Deletion for a Versioning File System", 2005.
- [71] Ara, A., et al.: A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems. *IEEE Access* 5, 12601–12617 (2017).
- [72] H. Tao and W. Peiran, "Preference-Based Privacy Protection Mechanism for the Internet of Things," 2010 Third International Symposium on Information Science and Engineering, 2010.
- [73] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, Oct. 2013.
- [74] G. Zyskind, O. Nathan, and A. sandy Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *2015 IEEE Security and Privacy Workshops*, 2015.
- [75] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT targetdriven applications," *Computers & Security*, vol. 37, pp. 111–123, 2013.
- [76] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. Aalborg, Denmark: River Publishers, 2013, pp. 22–23.

- [77] C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, G. Vassilacopoulos, Enabling data protection through pki encryption in iot m-health devices, in: 2012 IEEE 12th International Conference on Bioinformatics Bioengineering, BIBE, 2012, pp. 25–29.
- [78] K.T. Nguyen , M. Laurent , N. Oualha , Survey on secure communication protocols for the internet of things, Ad Hoc Netw. (2015) .
- [79] K.K. Venkatasubramanian, A. Banerjee, S.K. Gupta, et al., Ekg-based key agreement in body sensor networks, in: INFOCOM Workshops 2008, IEEE, IEEE, 2008, pp. 1–6.
- [80] D. Gessner, A. Olivereau, A. S. Segura, and A. Serbanati, “Trustworthy infrastructure services for a secure and privacyrespecting internet of things,” in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom '12*, pp. 998–1003, June 2012.
- [81] R. Bonetto , N. Bui , V. Lakkundi , A . Olivereau , A . Serbanati , M. Rossi , Secure communication for smart iot objects: Protocol stacks, use cases and practical examples, in: World of Wireless, Mobile and Multimedia Networks (WoW- MoM), 2012 IEEE International Symposium on a, IEEE, 2012, pp. 1–7 .

- [82] S.G. Weber , L.A. Martucci , S. Ries , M. Mühlhäuser , Towards trustworthy identity and access management for the future internet, in: The 4th International Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS 2010) co-located with the Internet of Things 2010 Conference, November, 2010 .
- [83] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, “A comprehensive approach to privacy in the cloud-based Internet of Things,” *Future Generation Computer Systems*, vol. 56, pp. 701–718, 2016.
- [84] L. González-Manzano, J. M. D. Fuentes, S. Pastrana, P. Peris-Lopez, and L. Hernández-Encinas, “PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things,” *Journal of Network and Computer Applications*, vol. 71, pp. 59–71, 2016.
- [85] L. Shen, Y. Zhang, and J. Gu, “Development Trend of IPv6-based Information Security Products in Network Layer of IOT”, 2012.
- [86] “IPv6 advantages for IoT,” *IPv6 advantages for IoT | IoT6.eu*. [Online]. Available: https://iot6.eu/ipv6_advantages_for_iot. [Accessed: 12-Nov-2019]
- [87] A. Juels, R. L. Rivest, and M. Szydlo, “The blocker tag. Proceedings of the 10th ACM conference on Computer and communication security - CCS '03”, 2003. doi:10.1145/948109.948126

- [88] X. Yi, Y. Liang, E. Huerta-Sanchez, X. Jin, Z. X. P. Cuo, J. E. Pool, X. Xu, H. Jiang, N. Vinckenbosch, T. S. Korneliussen, H. Zheng, T. Liu, W. He, K. Li, R. Luo, X. Nie, H. Wu, M. Zhao, H. Cao, J. Zou, Y. Shan, S. Li, Q. Yang, Asan, P. Ni, G. Tian, J. Xu, X. Liu, T. Jiang, R. Wu, G. Zhou, M. Tang, J. Qin, T. Wang, S. Feng, G. Li, Huasang, J. Luosang, W. Wang, F. Chen, Y. Wang, X. Zheng, Z. Li, Z. Bianba, G. Yang, X. Wang, S. Tang, G. Gao, Y. Chen, Z. Luo, L. Gusang, Z. Cao, Q. Zhang, W. Ouyang, X. Ren, H. Liang, H. Zheng, Y. Huang, J. Li, L. Bolund, K. Kristiansen, Y. Li, Y. Zhang, X. Zhang, R. Li, S. Li, H. Yang, R. Nielsen, J. Wang, and J. Wang, "Sequencing of 50 Human Exomes Reveals Adaptation to High Altitude," *Science*, vol. 329, no. 5987, pp. 75–78, Jan. 2010.
- [89] Z. Mahmood, H. Ning, and A. Ghafoor, "Lightweight Two-Level Session Key Management for End User Authentication in Internet of Things," *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016.
- [90] N. Li, D. Liu, and S. Nepal, "Lightweight Mutual Authentication for IoT and Its Applications," *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359–370, Jan. 2017.

- [91] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," 2005.
- [92] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668, 2012.
- [93] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," *Advances in Cryptology - EUROCRYPT 2004 Lecture Notes in Computer Science*, pp. 506–522, 2004.
- [94] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.
- [95] A. A. A. Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: a survey," *International Journal of Information Technology*, vol. 10, no. 2, pp. 189–200, 2018.
- [96] N. Fabiano, "The Internet of Things: Establishing Privacy Standards Through Privacy by Design," *Cutter IT J.*, vol. 26, no. 8, 2013; [www.cutter.com/article/internet-things-establishing-privacy standards-through-privacy-design-417276](http://www.cutter.com/article/internet-things-establishing-privacy-standards-through-privacy-design-417276).

- [97] “The Seven Foundational Principles,” *Ryerson University*. [Online]. Available: <https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/>. [Accessed: 18-Sep-2019].
- [98] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, “The Quest for Privacy in the Internet of Things,” *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36–45, 2016.
- [99] R. Piyare, M. Tazi “Bluetooth Based Home Automation System Using Cell Phone”, 2011 IEEE 15th International Symposium on Consumer Electronics.
- [100] Dhakad Kunal, Dhake Tushar, Undegaonkar Pooja, Zope Vaibhav, Vinay Lodha, “Smart Home Automation using IOT” in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2016
- [101] Shrestha, Bijay & Mali, Suman & Joseph, Asha & Singh, K. & Raj, Kiran. (2017). Web and Android based Automation using IoT. International Journal of Latest Technology in Engineering, Management & Applied Science. VI. 23-26.
- [102] Z. Yan, P. Zhang & A. Vasilakos, A Survey on Trust Management for Internet of Things, *Journal of Network and Computer Applications*, Elsevier, June 2014.

- [103] P. F. Pires, E. Cavalcante, T. Barros, F. C. Delicato, T. Batista, and B. Costa, "A Platform for Integrating Physical Devices in the Internet of Things," 2014 12th IEEE International Conference on Embedded and Ubiquitous Computing, 2014.
- [104] de Carvalho Silva, Jonathan & Rodrigues, Joel & Saleem, Kashif & Kozlov, Sergei & Rabelo, Ricardo. (2019). M4DN.IoT -A Networks and Devices Management Platform for Internet of Things. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2909436.
- [105] J. Clawson, J. Pater, A. Miller, E. Mynatt and L. Mamykina, "No longer wearing", *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15*, 2015. Available: 10.1145/2750858.2807554.
- [106] D. Epstein, M. Caraway, C. Johnston, A. Ping, J. Fogarty and S. Munson, "Beyond Abandonment to Next Steps", *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016. Available: 10.1145/2858036.2858045.
- [107] *InternetSociety.org*, 2020. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf.

- [108] "Double-Digit Growth Expected in the Smart Home Market, Says IDC", *IDC: The premier global market intelligence company*, 2020. [Online]. Available: <https://www.idc.com/getdoc.jsp?containerId=prUS44971219>.
- [109] "People say they care about privacy, but they continue to buy devices that can spy on them," *Vox*, 2020. [Online]. Available: <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security>.
- [110] S. Zheng, N. Apthorpe, M. Chetty and N. Feamster, "User Perceptions of Smart Home IoT Privacy", *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no., pp. 1-20, 2018. Available: 10.1145/3274469.
- [111] M. Tillman and B. O'Boyle, "What are Google Home, Home Max, Nest Mini, Nest Hub, and Nest Hub Max and what can they do?", *Pocket-lint*, 2020. [Online]. Available: <https://www.pocket-lint.com/smart-home/news/google/137665-what-is-google-home-what-can-it-do-and-how-does-it-work>.

Appendix A



Florida Institute of Technology
Institutional Review Board

Notice of Expedited Review Status Certificate of Clearance for Human Participants Research

Principal Investigator: Leena Alghamdi
Date: November 14, 2019
IRB Number: 19-175
Study Title: A Web-based User Interface for the Internet of Things

Your research protocol was reviewed and **approved** by the IRB Chairperson. Per federal regulations, 45 CFR 46.110, your study has been determined to involve no more than minimal risk for human subjects. Federal regulations define minimal risk to mean that the probability and magnitude of harm are no more than would be expected in the daily life of a normal, healthy person.

Unless you have requested a waiver of consent, participants must sign a consent form, and the IRB requires you give each participant a copy of the consent form for their records. For online surveys, please advise participants to print out the consent screen for their files.

All data, which may include signed consent form documents, must be retained in a locked file cabinet for a minimum of three years (six if HIPAA applies) past the completion of this research. Any links to the identification of participants should be maintained on a password-protected computer if electronic information is used. Access to data is limited to authorized individuals listed as key study personnel.

Prompt reporting to the IRB is required in the following conditions:

- Procedural changes increasing the risk to participants or significantly affecting the conduct of the study
- All adverse or unanticipated experiences or events that may have real or potential unfavorable implications for participants
- New information that may adversely affect the safety of participants or the conduct of the study.

This study is approved for one year from the above date. If data collection continues past this date, a Protocol Renewal Form must be submitted.

High Tech with a Human Touch™

150 West University Boulevard, Melbourne, FL 32901-6975 • (321) 674-7316

Appendix B

Perceptions of a Web-based User-Interface for IoT Device Management.

This study is designed to explore a Web-based User Interface for Internet of Things devices that will help in enabling IoT users to manage all their devices from one platform. Please take a few moments to use the website based on the following steps:

- Click on the following link to our interface: <http://iotprivacycontrol.com/>
- After you open the website, click on the **Account** button to sign in as **Bob Smith**.
- Please use the following information to sign in:
Username:Bob.smith@gmail.com
Password:Bobsmith.2019
- After you have signed in as Bob Smith, please **add** a smart door-lock device.

Once you are logged in, please complete the following tasks and the questionnaire:

Based on the website <http://iotprivacycontrol.com/>, please complete the following tasks and answer the following questions:

1. **Task 1:** How many IoT devices are currently connected to this website?
2. **Task 2:** Turn on the sensor readings function for the Temperature and pressure sensor (**BMP180**).

How many temperature readings are currently listed for the BMP180 Temperature and Pressure sensor?

3. **Task 3:** What was the temperature reading at 07:28:44 on 10/24/2019?

4. What is your age?

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65+

5. What is the highest level of education you have completed?

- ☐ High school
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Ph.D. or higher
- ☐ Other (please specify)

6. In general, how concerned you about privacy in your daily life with the following examples are:

	Not at all	A little concerned	Somewhat concerned	Very concerned
People knowing your private and personal information				
Walking in a public place which is full of sensors such as, private security camera, traffic microwave radar sensor, etc.				
To be in the background of photos that are taken by strangers				
To be in the foreground of photos that are taken by strangers				

Other (please specify)

7. Which Internet of Things (IoT) device(s) do you own. Select all that apply.

- ☐ Smart phone
- ☐ Smart watch
- ☐ Activity tracker
- ☐ Smart refrigerator
- ☐ Smart speaker (e.g., Amazon Echo, Google Alexa, etc.)
- ☐ Smart thermostat
- ☐ Smart TV
- ☐ None
- ☐ Other (please specify)

8. How many hours per week do you use IoT devices? (if you do not have an IoT device please choose zero for all)

	0	4 - 6 hours	7 - 10 hours	11 - 14 hours	15 - 20 hours	More than 20 hours
At home						
At work						
Other						

9. For what purposes do you use IoT devices? Select all that apply.

- ☐ Smart Home
- ☐ Smart energy monitoring system
- ☐ Vehicle Tracking
- ☐ Entertainment
- ☐ Lifestyle
- ☐ Health monitoring
- ☐ None (do not have an IoT device)
- ☐ Other (please specify)

10. Rate how important privacy (e.g., protecting your personal information) is to you when you are using smart devices.

Very important	Somewhat important	Neutral	Somewhat unimportant	Unimportant

11. Rate how important convenience (e.g., completing a task such as, increasing the thermostat temperature) is to you when you are using smart devices.

Very important	Somewhat important	Neutral	Somewhat unimportant	Very unimportant

12. If you were using these IoT devices (Smart Thermostat, Smart Tv, and Smart phone) at the same time, what type of information do you think would be captured by these devices? Select all that apply.

- ☐ Personal Information (e.g., name, address, bank information, etc.)
- ☐ Biometric Information (e.g., Fingerprint, Facial Pattern, Voice, etc.)
- ☐ Location Information
- ☐ Weather Information (e.g., temperature degree)
- ☐ Audio recordings
- ☐ Video recordings
- ☐ Health Information (e.g, medical histories, test and laboratory results, mental health conditions, etc.)
- ☐ Other (please specify)

13. Which of the following applications do you use to manage your IoT devices?

- ☐ Wink
- ☐ SimpliSafe Home Security
- ☐ Yonomi
- ☐ ADT Control
- ☐ Olisto
- ☐ None
- ☐ Do not have an IoT device
- ☐ Other (please specify)

14. How important to you are each of the following actions in terms of protecting your personal information that is captured by IoT devices:

	Very important	Somewhat important	Neutral	Somewhat unimportant	Unimportant
Enabling you to control what information is being collected about you by IoT devices.					
Informing you when personal information about you is being collected by IoT devices					
Requesting your permission to collect your information by IoT devices before it is collected.					

15. Assume you are at your friend's house and they have a security camera which is recording audio and video that is kept for one week. How important to you are each of the following actions in terms of protecting your personal information that is captured by that IoT device.

	Very important	Somewhat important	Neutral	Somewhat unimportant	Unimportant
I would be very careful of what I do (e.g, act differently).					
I would be very careful of what I say.					
I would sit in blind spots where I am not captured by the security camera.					
I would use technical methods if applicable (e.g, applications, websites) to hide my identity.					

16. Rate the extent to which you agree or disagree with the following actions and statements if you were in this situation: You live in a Smart home that contains different IoT devices and sensors which are: Smart Tv, Smart light, Smart Thermostat, and Smart watch) that capture various types of your information (e.g., your personal information, room temperature degree, your heart rate, your TV watching preferences, etc.), and you want to manage your devices, and reduce the risk of privacy breaching:

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
I am concerned about the privacy of data sensed about me when using IoT devices.					
I prefer to use ONE platform (e.g., website) to manage all my IoT devices.					
I prefer to use website to manage my IoT devices rather than a particular application.					
For each device I prefer to use its related application for management purposes.					
I prefer to implement centralized monitoring for my IoT devices to manage privacy and security issues.					
I prefer to update my IoT devices with regular software updates.					

17. Based on your experience in our website <http://iotprivacycontrol.com/>, how satisfied are you with the following.

	Very satisfied	Somewhat satisfied	Neither satisfied nor dissatisfied	Somewhat dissatisfied	Very dissatisfied
Website organization					
Ease of website navigation					
User friendly interface					

18. Rank the following statements in order of importance from 1 to 3, where 1 is most important to you and 3 is least important to you.

- Governments should provide new rules and laws to regulate IoT devices to protect our privacy when using them.
- IoT devices' manufacturers need to provide software updates and new features constantly for IoT devices to protect our privacy when using them.
- IoT devices' users need to use platforms (e.g., websites and applications) to manage their IoT devices to protect their privacy.