Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia

Omar Almutairi[1]
Computer Science Department
Shaqra University, Shaqra
Saudi Arabia

Khalid Almarhabi[2]
Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University
Makkah, Saudi Arabia

***Abstract*—One of the fastest and most developing technologies around the globe is the Internet of things (IoT). The research questions in this study focus on the security and privacy challenges for a smart home environment. The geographical region of Saudi Arabia is the selected boundary for the study. The study is focused on finding the problems associated with the Smart Home adaption in Saudi Arabia. However, there is a large phase shift, which is seen towards the increase of threats in smart homes. It is believed that the awareness by humans towards the use of these devices. The level of security offered by the devices, is one of the factors for these threats and privacy issues. This research targets to identify all the facts that can be discarded towards adaption of Smart Homes. It is desirable that a quantitative methodology must be implemented for identification of the population under threat due to IoT devices in smart homes. The views of the users are the major input values to trace the problems. The expected results from this research will provide all the factors which can be improved and provided with proper solution to avoid any security or privacy threats in the Saudi Arabian realm.**

***Keywords*—Smart home; IoT; Saudi Arabia; security; privacy; issues; demographic; perception; consumer**

I. Introduction

The Internet of things (IoT) refers to the connection of physical objects that are created with the help of sensors and connected to a local area network. The devices exchange data with the centralized database server systems, which in return are capable of processing the information passed on from these devices. The decision-making and the business flow take place with the help of these decisions and the analysis done by the combination of the devices and servers. The evolution of such devices started in 1982, when a Coca-Cola vending machine was able to send information about skates inventory and sales over the Internet at Carnegie Mellon University [1].

The ecosystem of the IoT-based devices is comprised of five basic elements [2]. First and foremost are the sensing and embedding components. These devices are loaded with any kind of sensor to provide specific functionality. Second, another class of elements is the connectivity and networking components that empower the devices to communicate with a centralized communication unit, or with a server, more specifically. Improvement in the use of IOT leads to adaption of cloud technologies. The IOT Cloud becomes the third important element in this context. The usage and the information for any device that is empowered with IOT-based learning is recorded in the cloud. The management of the data is done in the cloud. However, the analysis is done with the help of sophisticated analytics and data management services. The endpoint of the realm is comprised of the end user devices that have an interface for communication.

There is a strong change observed towards the digital environment in today's challenging world. Practically everything is sensed and recorded to derive conclusions and define business processes [3]. The integration of all the processes is done with the help of Internet- and sensor-based devices. It is really an important improvement, which is required at this point in time. However, it also has its own drawbacks. There is a strong requirement of trusted frameworks for the smooth working of this drastic digital upgradation. According to the Vision 2030 of Saudi Arabia, the adaption of digitization is one of the major factors. The use of Internet and communications technology to improve the quality of living and to facilitate the citizens is indeed one of the most important aspects towards use of IOT [4]. Various projects going under the National Committee for Digital Transformation in Saudi Arabia since 2006 have started achieving national digitization. The most promising factor for this relates to digital health, education, e-commerce and smart cities, including smart homes. A promising study conducted by [5] reveals the fact that even the citizens as well as the residents are looking forward to improvements in the quality of the standard of living, with the use of smart homes and IOT-based devices.

II. The Smart Home Environment

The general thinking that arises in the mind about smart homes is that they are comprised of security and surveillance systems. However, these systems are not enough to make a home smart. A taxonomy of the smart home services was presented by [6]. The main categories in which a smart home can be expected to work are comprised of detection of health conditions, storing and retrieving multimedia information, security and surveillance, and, finally, device monitoring for energy conservation. The broader classification of a smart home can include safety, energy consumption management, and lifestyle support. The ultimate global extinction of nonrenewable resources of energy has led to the necessity of identifying renewable sources of energy and reducing the usage of energy consumption. Smart homes are providing a new era for the conservation of energy and supporting the cost of living of humanity.

The very first smart home device of its kind was developed in 1966–67, which was called ECHO-IV. The device was capable of managing shopping lists, controlling the temperature of the house and turning off certain appliances [7]. However, the device was not sold anywhere, but it laid the foundation of smart home units and research into the field.

The use of sensors and meters to pass along information using a network can be helpful for monitoring all the activities and assets remotely. Sophisticated techniques are integrated into smart homes to provide a large amount of information that is helpful for the maintenance and performance of predicted conditions. The use of persuasive technology given by [8] gives complete information about the future of smart home technology. The automation of any home for the conservation of energy can be really helpful in achieving goals, such as hydro-thermal, visual, air quality, and also plug loads usage [6].

The connectivity amongst various sensors, appliances, components and devices, with the help of a network education system, collectively creates a smart home environment. The remote access and monitoring can be done for the house with the help of these devices and observation. A centralized database-monitoring unit is responsible for recording all the observations and information about the system. On the same side, the devices are connected to provide smart energy management from remote locations, even if the owner is not present at the house [6]. The most important unit of a smart home is the network itself. The real-time exchange of information is done in such a way that the monitoring and decision-making can be done from remote locations. An advanced control system is good enough to provide these features in the smart home environment. Significant savings of 5%–15% energy consumption is predicted in the study, compiled by [9].

With the increasing charm of using a smart home, large numbers of vendors have started producing gadgets that are responsible for providing special features that are integrated with sensor-based devices. Some of the important organizations producing devices capable of providing smart home features include Apple Home, Google Home, Arduino Smart Homes, Raspberry Pi, ZigBee, etc. The integration of the services given by these companies provides smart home solutions. All the smart home devices are usually connected with the help of a network created within the home. The information that is recorded with the sensors is passed on via this network to the cloud of the organization. Once the information reaches the cloud, it is recorded and can be used for real-time monitoring and observations.

However, whenever it comes to network and information sharing, the most important part is the confidentiality and security of the information. A large number of data leaks in the previous year has revealed vulnerabilities in the sharing of information of an individual home over the network. The adaption of technology of smart homes is the need of the hour, but the fear of information security and illegal use of the information remains a big issue. The authorization of a validated user to access the information from the cloud for remote monitoring is indeed one of the most important factors responsible for safeguarding individual privacy. The potential loss of biometric information, such as voice samples, fingerprints, retina scans, etc., should be checked at every instance.

The Mirai Botnet Attack of October 2016 was one of a type of massive Distributed Denial of Services Attacks that sacrifice the information from millions of IOT devices. The result of such a sacrifice of information influenced millions of users whose businesses were relying on the services provided by Mirai. The organization placed the source code of Mirai Botnet on the Internet where it was sacrificed and the information from their servers was stolen and misused. With the increase in the popularity of the usage of IOT-based devices, the future of cyber security is still not clear for smart homes.

III. Security and Privacy in Smart Homes

When it comes to the security of a smart home, privacy concerns are on the highest acclivity. The success of smart homes depends on the challenges posed by the security issues. The use of electronic devices to safeguard the home is becoming popular nowadays. However, the dynamic networks created and the integration with the Internet of things devices make it challenging. Large numbers of devices are vulnerable to individual privacy, and make it very easy for the attacker with easy access, once he connects to a dynamic network [10]. Sometimes, the user of the smart home devices is responsible for yielding the space to such vulnerabilities. Incomplete knowledge about the use of such devices makes it easy for an attacker to create a threat towards individual security and policy concerns. An exponential rise seen in the frequency of attacks at such complex dynamic networks constitutes an alarming situation [11].

A. Information Storage

One of the most challenging situations is the collection of information from the devices on the vendor servers or cloud storage. The data from the smart home reaches the cloud storage of third parties; this data can be confidential, as well as critical, and may yield to a security breach. Two billion records were once sacrificed from a Chinese agency that ran an IOT-based platform [12]. The geolocation and the statistics, including the precise information of the household, may lead to burglary opportunities. There are chances for various devices rendering, based on the circumstantial availability of the data.

B. Copyright Infringement

During the initial setup of devices integrated with the smart home, terms and conditions are accepted, along with the provisioning of voice samples and sometimes-biometric recognitions [13]. This can result in a major threat towards individual privacy and concern. Even private communications may sometimes prove not to be private, since they are monitored and captured with the help of smart devices [14]. The communications are synchronized with some remote servers that are inaccessible, which in turn compromises the privacy policy of individual data.

C. Attack Probabilities

Generally, once, when a user accesses the internal network, and the devices that are active record observations, it is

probably likely that vulnerability inside the network can occur. The attacker tries to gain access over simple devices, which in turn can provide further access to a larger number of information channels throughout the network. A single vulnerability at a weaker device can be a big threat to the entire network of smart home devices. The ability to track family member habits/behavior or location after getting access to some vulnerable home devices is yet another possibility that can arise. An official watchdog was found once in 2017 to instruct parents to destroy Cayla, a doll [15]. The deciphered reason showed that one of the Bluetooth devices was compromised on security breaches by an attacker who used the doll to talk with the child playing with it.

D. Physical Security

One of the most important and key factors for the IOT-based devices is physical security. The use of low quality sensors and cheap digital circuits can be harmful and hazardous to the devices that are implanted inside the house [16]. The malfunctioning of these devices can lead to improper readings, such as for the location, and addressing of the desired information. It is also likely that these devices are weathered very easily with the normal fluctuation of temperature and moisture conditions. It is also worth noting that such cheap devices are available in the market in a variety. However, there has to be a trust with all the manufacturers and the devices that are implanted inside the home to provide smart home services.

Yet another consequence for the use of such devices is the possibility that they can provide dangerous situations of fire and destruction. Since a major portion of each device is controlled with the help of electric signals, there are chances of electric malfunction due to the use of low quality manufacturing material or doped semiconducting material that can be harmful. The handling of these gadgets requires special training, and the deployment of these devices needs an experienced workforce. However, the lack of such a workforce and an inexperienced staff can also lead to issues created inside the circuits.

E. Lack of Control and Awareness

The smart home devices and gadgets that are implanted at any house require sophisticated handling and a managing skillset. These devices are delicate and need special attention for handling. Some of the precautions that are required to handle these devices are comprised of the following facts:

1) The devices should be planted at a considerable height, out of the reach of children [17].

2) They should be located at a place where rodents and moles cannot destroy or damage the cabling or wiring of the system.

3) There are several devices that require restricted moisture conditions or temperature variations [18]. It should really be emphasized that the location of such devices having sensitive sensors should be away from any underlying physical conditions that do not meet the requirements.

4) Installation of the devices should be done precisely, and all the connections as well as the cabling must be tested and checked at proper times. The maintenance of such systems should be done at regular intervals to assure proper working of the smart home.

5) The most important part for using such devices is proper training and awareness. All the users who are administering or using the devices should be properly dedicated for such use [19]. They must undergo proper training from an experienced organizational professional for the code of conduct and usage.

F. Integrity of Data

The most important concern for the use of smart home devices is the data. Care should be taken to safeguard the privacy of individuals. As a safety measure, the end user must know the data that is travelling in the network that is using the devices. The privacy of the data should not be compromised at any instance. It is also recommended that the end user should be a technical and technology-efficient person, to handle the information flow and its security. While there are many chances for any type of data breaching or hacker attacks, it is very important to decide which data should be flowing in the network and control the data as per the privacy concerns.

IV. Related Works – IoT in Saudi Arabia

For the growth of the nation, and the Vision 2030 of Saudi Arabia, there is a big scope for adaption of smart homes in the country. To improve the quality of living and facilitate the citizens, digital transformation is going on in every sector of government as well as private organizations. Large numbers of sectors are targeting towards improvement in IOT-based devices, which includes environmental monitoring, infrastructure management, manufacturing units, transportation, medical health care and home automation. The Communication and Information Technology Commission (CITC) in the Kingdom of Saudi Arabia have given certain guidelines based on which integration of IOT devices is going ahead for various sectors in the country [20]. There are certain standards that are followed as per the guidelines generated by CITC.

However, a descriptive survey was conducted by [21], which reflected the special requirements before the application of IOT. The survey also conducted a very strong screening method along with certain analyses to identify the role of the data centers in the country for minimizing the cybercrimes and the risks. It is clear from the above section that adaptability of smart homes in a country depends entirely upon the perception of the people and various other factors. To reduce the risk and the level of cyber threats towards the information and data, a country is expected to implement powerful decisions. Proper measures for the adaptability of smart homes in any country should be taken prior to the adaption. It is clear that the seriousness of the use of IOT, in the Saudi Arabian region, can be addressed with the help of educating the users, providing security measures, managing information and privacy, handling cyber situations, and, finally, identifying the required security requirements [21].

The use of integrated technology and embedded devices for providing smart homes will open the path for cyber criminals and hackers, from which the misuse of information is more likely to happen. In contrast with the facilitation of smart

homes, cybercrimes and other non-ethical data privacy issues are more likely to occur. Internet-connected devices are going to facilitate the user on one side, but can be more dangerous at the other end [21]. As presented in one of the studies by [22], approximately 50 billion devices are connected across the globe, through which the data is travelling. This number is going to rise significantly in the near future. The IOT model for maintaining security and privacy requires specific attention to security management, including identity management as well as data ownership. There has been an inverse relationship as identified by [21] between the awareness as the former part, and readiness as the later part, in the domain of IOT and cybercrimes.

A large number of communities and cities are planning for growth and development in the kingdom of Saudi Arabia towards the proper planning and adaption of the smart city. The correlation between smart city and smart homes is really clear, and the development of the idea entirely depends upon the adaptability of smart homes in the country [23]. Large numbers of wireless sensors, in association with technology-driven routines and mechanisms, empower the uplifting of the living standards for an individual in his house. The IOT conference, organized by [24], showcases the use of IOT in Saudi Arabia. The conference also leads to case studies as well as to smart solutions that are an integral part of the Vision 2030 of the Kingdom and beyond. The adaption of IOT and its allied services are also portrayed in the NEOM City project of Saudi Arabia [23].

It has also been identified that approximately 81% of businesses in Saudi Arabia have already started using IOT and its allied technologies [25]. Big players in the software industry, such as IBM and Oracle, have also entered the race. The IOT harp for these organizations has released special devices and sophisticated software in the Middle East region for adaptability. With the use of IOT in business, it can be considered that the adaptability of smart homes is not going to take a lot of time. It is further expected that the Saudi Arabian market for IOT devices and their adaptability is going to exceed $3 billion in subsequent years [26]. It is also expected that around 11.3 million devices will be having the connectivity towards the emerging technologies, which will be making use of IOT techniques enabled with the help of wireless sensor networks, embedded systems, persuasive computing, etc. However, along with the upcoming growth and advancement in technology, the risks are also increasing in cyber security. Technology will be more vulnerable to cybercrimes and attackers who hack valuable information and present hazards to individual privacy by data breaching.

V. Research Methodology

Under research methodology, processes for data collection will be described. This section of the research will also delve into illustrating the adopted methodology for the proposed validation. The function of the quantitative research method is explored in this research to investigate the consumers' perception about smart home security and privacy in Saudi Arabia, encompassing usage as well as terminology. The selection and choice of this approach was informed by its capacity in determining not only opinions but also attributes of participants.

We used a survey to evaluate the respondents' concerns about the security and privacy of smart home devices in Saudi Arabia. The aim of this research is to identify security and privacy challenges facing smart homes, followed by an investigation of the users' privacy and security concerns of smart homes. In addition, this research also attempts to recognize privacy security mitigation actions that users take to protect themselves, and to know the opinions of users about those responsible for the privacy and security of smart home devices.

The questionnaire was developed into five distinct segments, comprised of demographic information, security and privacy concerns, mitigation actions, usage of smart home devices, and responsibilities. Under the demographic segment, elements such as age, job status, sex, education, and organization are covered. The second section contains smart home device types and numbers, the time period for using the devices, data types of smart homes, and the security classification level and sensitivity of data-based consumer opinion. The third part focuses on the security and privacy issues facing the smart home environment and consumers driven from the concerns that are discussed in section two of this paper.

The fourth part concerns the participants' behavior and action to mitigate risk and protect consumers and their smart home devices. Finally, the last part covers the roles and responsibilities of those involved in the implementation of smart home devices, based on the consumers' point of view. The survey exploits the Liker Scale, which is calibrated with measurements of 1 to 5, coinciding with (1) Agree (2) Disagree (3) strongly Agree (4) Strongly Disagree (5) Neutral. Different but appropriate software is used in analyzing research data and in completing the survey.

A. Data Awareness

Due to the issue of limited space in data presentation and discussion, much attention will be drawn towards relevant results that will be generated under this section with respect to data analytics. Our sample size was more than 210 participants, including 205 participants who already use smart home devices; 72% of the total number of participants use between two to five types of smart home devices at the same time, and 69% of the total number of participants have used smart home devices for more than three years, as shown in Figure 1. In terms of education level, the majority of the participants have bachelor's degrees, representing 51%, and 23.5% have a master's degree. In terms of the location of the participants, 95.4% live in Saudi Arabia, and, because they are the only target audience, other participant's results are ignored.

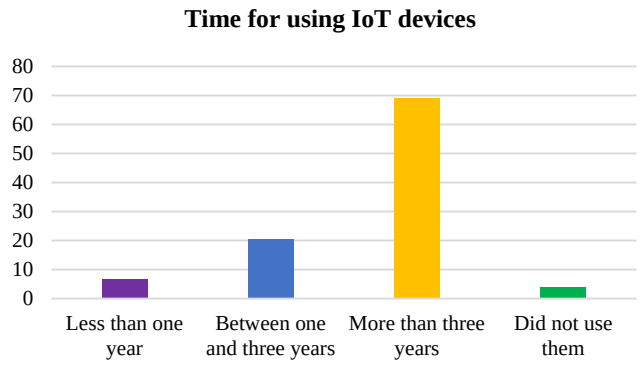

Fig. 1. Age Group based Mapping for use of IoT Devices.

In terms of demographic information, our study shows that the age group from 26 to 35 years old is the largest in our study, representing 44.9% of the total number of participants, followed by the age group from 36 to 45 years old at 35.2%. The type of living of the respondents shows that people living with their family were the largest groups in our study, by 96.9%, and 2.6% live alone and 0.5% live with friends. Despite the low number of female participants (30.6% of the total number), this study indicates that there exists a percentage in terms of consumer perception between males and females.

In terms of the purpose of using smart home devices, the majority of participants, 55.1%, use smart home devices for entertainment and relaxation proposes, while 51% of the total number of participants use smart home devices equally to receive technical assistance and to keep up-to-date with the development of technologies around the world. The result of the survey shows that most of the participants, 79.1%, are concerned about their data used in these devices. Consumers are worried about how to control and secure the data, which indicates the importance of this research, taking care of the causes and solutions, and providing adequate guidance and training.

B. Discussions

This research aims to investigation smart home security and privacy issues based on the consumers' perception in Saudi Arabia. Therefore, this section is classified into five main categories: privacy issues, security concerns, awareness and knowledge, consumer's mitigations, and stakeholder responsibilities. The main research questions to be answered in this section are these:

1) What are smart home users' privacy and security concerns in Saudi Arabia?

2) What privacy/security mitigation actions do users take in Saudi Arabia?

3) Who do users believe is responsible for the privacy and security of their smart home devices?

C. Privacy Issues

Proliferation of intelligent systems into the day-to-day life of people' homes stems from the rapid and robust development of the Internet of Things. But, the increasing utilization of these technologies has generated concern regarding the collection, handling, and usage of sensitive data. Issues have been complicated by the fact that the function of privacy continues to be unexplored within the context of smart home usage. It is noteworthy that information privacy denotes the capacity of an individual to control their personal information. Achieving such a goal is increasingly becoming difficult, given the advancement of digital technologies. Different sensing technologies are explored in smart home devices and in providing services. By collecting colossal amounts of data, these sensors provide services to users by allowing these data to be processed and interpreted. However, a combination of the collected personal data and exploitation of internet-connected devices predisposes residents to emerging security and privacy risks.

Based on the survey results, 79.7% of the respondents are worried about the statutes of the privacy and security. Their data can be spread without their knowledge. There are many parties through which data can be spread, such as smart home device manufacturers and Internet service providers. Aspects of control and certainty are indicated as necessities for human beings, therefore, the absence of these elements results in suffering [27]. Our result shows that 78.8% of participants are afraid of smart home device manufacturers who can access their private data and monitor user behavior. In addition, when participants were asked about privacy violation by intrusions on their privacy, even if any third parties had obtained consent from users regarding the authority to access some consumer data, they replied as follows, and as shown in Figure 2: 47.8% strongly agreed, 30.9% agree, 11.2% neutral, 8.4% disagree, and 1.4% strongly disagree.

One reason for the growing consumer concern is the weakness of their knowledge about data collected and when and how it is gathering. Because of low levels of public awareness, functionality continues to be the primary focus of many users. Therefore, they fail to interrogate how these services are being provided [28]. The second reason may be due to the weakness of the standards and policies of protecting user privacy that need to be fulfilled by smart home device manufacturers, or which perhaps exist but are not present in the correct and understandable manner. Regulations and standards should be implemented in the products and services provided by companies, whether they are local or global, such as by the General Data Protection Regulation (GDPR). Privacy policy must be provided by vendors of smart home devices, as such policy is regarded as an internal statement designed to guide an entity or organization in handling and managing personal information. As a matter of fact, it is targeted at the recipients of personal information. Employees are instructed on the correct approaches of collecting and using data as sanctioned by the privacy policy on the collection and the use of the data.

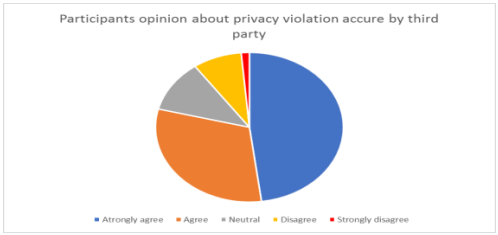

Fig. 2. Trust Percentage on Privacy Violation by ISP.

The result shows that 41.3% of the respondents trust the Internet service provider, while 27.6% express concerns about their data. Government monitoring of the performance of Internet service providers to ensure quality may increase user trust to use smart home devices. In Saudi Arabia, the regulatory framework for Cloud Computing is established to protect user data, which must remain stored in cloud services within the Kingdom of Saudi Arabia [29]. In general, privacy is one of the main concerns of people and of whether users are concerned over their inability to control personal and private information. Such concerns are measured to make users aware of the risk of invasion, thus minimizing privacy issues. Applying this to the context of smart home devices will make users shy away from adopting these technologies, out of fear of possible breaches to their privacy.

D. Security Concerns

The fact that a security technology is easier to use might hint to the fact that it is easier to be intercepted or compromised by criminal minds. Each feature of a device or service is laced with a possible risk for attack as well as potential for failure. Within the smart home environments, it is difficult to design perfect watertight security. This is because of the prevailing heterogeneous ecosystem defined by a plethora of devices as well as services. Matters are complicated further by the fact that such systems, apart from having limited security, are also affected by weal capacities in terms of segments such as battery and CPU. Consequently, the provided services depend on remote infrastructures including cloud storage and analytics. It is estimated that 80% of IoT devices are open to a myriad of attacks [30]. As a matter of fact, linking traditionally 'stand-alone' smart devices, such as appliances, lights, and locks, poses innumerable cyber security risks. Some of the commonplace cyber security attacks and threats on Smart Home devices comprise: Man-in-the-middle, Device hijacking, Permanent Denial of Service (PDoS), Data and identity theft, and Distributed Denial of Service (DDoS).

According to our survey, most of the participant, 80.7%, are anxious of security vulnerabilities that exist or are likely to exist in smart home devices, including attacks on vendors. Security vulnerability refers to a vulnerability which can be abused by a threat actor, including attackers, by crossing privilege boundaries with the aim of performing unauthorized actions within the context of a computer system. In order to exploit an area of weakness, an attacker must leverage at least one applicable technique or tool that is connected to the identified weakness in the system. In this regard, vulnerabilities are referred to as the attack surface. The seriousness of the vulnerabilities is especially pronounced when they are discovered but have not yet been updated or fixed, such as in the case of a zero-day attack, which is a point of exploitation on the computer software that remains hidden from those who are supposed to alleviate existing vulnerabilities, such as the vendor of the vulnerable software. Unless these points of weakness are minimized, hackers can take advantage of them to disorient and compromise computer data, programs, networks, or additional computers.

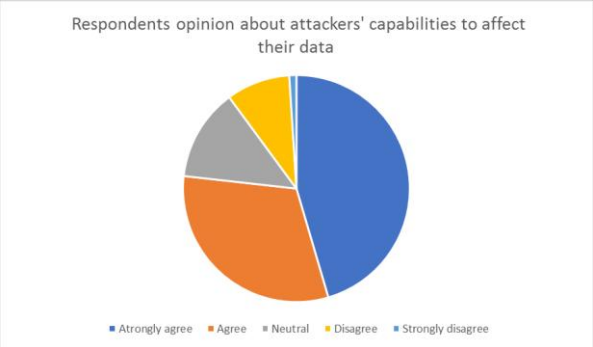

Fig. 3. Percentage of Opinion for Vulnerability towards Data.

When respondents were asked about believing that attackers have capabilities that enable them to access user data illegally and negatively influence it, the respondents replied as follows, and as shown in Figure 3: 45% strongly agreed, 31.4% agree, 12.6% neutral, 9.3% disagree, and 1.4% strongly disagree. The high percentages may reflect feelings of insecurity, especially since much of their data—such as medical, financial, and other data—can be accessed through smart home devices. The participants feel that the data they are most scared of being leaked are financial data, by 75.1%, then family data by 68.5%, then video data by 66.7%, then national ID number by 53.1%. On the other hand, smart home device performance monitoring data received the lowest level of importance, based on the user's perspective, with an 8.5% rate.

Some vendors may use what is known as off-the-shelf software or commercial off-the-shelf, which are products that are highlighted as packaged solutions with attributes that are designed to meet the needs of the purchasing organization, as opposed to bespoke, or custom-made, solutions. The disaster is that the breach of such software or platform could affect all companies and users who are working on it, as happened with the Solar Winds company in the United States recently, and this is what most of the participants in the questionnaire believe, with a percentage of 64.3%. It is evidently clear that cybercriminals are on a hunt for IoT-related points of weakness that are especially lacing new devices, and this communicates the need for adequate security to be implemented at the design phase and along the different stages, up to the deployment phase of the device. What this may hint at is the fact that vulnerability management associated with IoT devices has an important function in reducing attack openings.

In general, security is one of the biggest challenges facing smart home devices. Most individuals watch favorite programs and film Smart TV, and even connect baby monitors to a home network, but, in many cases, they do this in total disregard of their devices' security. It should be noted that one single mistake can give way to a hacker. While on the network, people can gain access and connection to other devices. This means they can abuse the accessed personal data information of voice recording and video, including streaming and storage. Security is an important part that needs to be addressed by all parties, as discussed in the next section, on responsibility.

E. Awareness and Knowledge

Awareness among consumers concerning privacy and cybersecurity issues is underlined as a crucial factor of organizations' posture on cybersecurity. It is understood that an adequately informed consumer regarding key issues related to cybersecurity will stand a better chance of defending and guarding against social engineering as well as other attacks. In order to appropriately develop IoT resources that will serve the communities better, the creation of a higher degree of awareness with regard to cybersecurity is required. This should go hand-in-hand with the training of users. This is the best approach, positioning consumers as active players and as a defensive layer within the structure of organization's security. Achieving this end requires initiatives aimed at educating and instructing the public with the primary aim of diminishing risks related to the IoT environment. The first step is to identify the status of security awareness regarding IOT vulnerabilities, and then design a program that includes best practices for increasing the level of awareness. In Australia, the government published and released.

The Code of Practice in August 2020 with the aim of strengthening the security of the Internet of Things for users. Both the Voluntary Code of Practice and The Code of Practice-Securing the Internet of Things (IoT) for consumers are established on 13 principles. However, our research found that 39.4% of respondents believe that cyberattacks are a fact and not an exaggeration, while 38% think it is not true, and 22% of respondents were neutral about this issue. This indicates the presence of partial awareness among the participating group, some of whom may not have previously been exposed to a cyberattack. In addition to the above, three-quarters of the respondents feel that they have sensitive data that needs protection. Reading instructions and training on the use of smart home devices is one of the most important practices that indicate increased awareness of the user, as the results have shown that 69% of the participants believe that reading the instructions and asking about them and how to use them safely is a necessity. In addition, 46% of respondents believe that insecure devices that do not give the user the authority to control and mange access to data in these devices should not be purchased. On the other hand, 50.7% of the participants follow news and technical posters related to the security of smart home devices, while 15% do not show any interest, as shown in Figure 4.

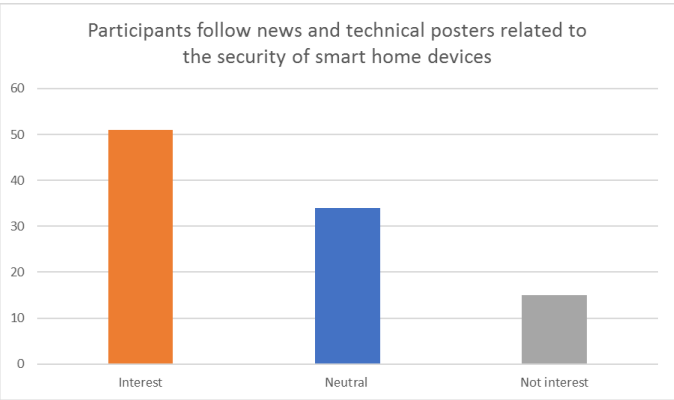

Fig. 4. Smart Home Security Adaption by Users.

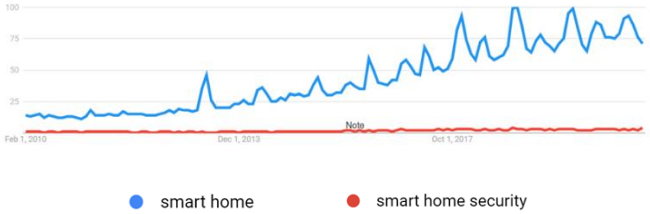

Fig. 5. Trends in 'Smart Home' & 'Smart Home Security'.

In Figure 5, comparison is made between the search terms 'smart home security' and 'smart home'. The aim here is to determine if users interested in adopting home automation technologies are equally keen on ensuring that their devices are secured. It should be noted, however, that this should not be misconstrued to mean that, in so doing, the research is aiming at a definitive statistic of trend. As a matter of fact, this is merely an approach that offers more insight into the content of the literature review. Assessments indicate that, while a focus on smart homes has risen significantly over the past 11 years, the attention given to the security of devices is still insignificant. This reality raises concern, since not all users are technologically oriented. Therefore, it is likely that these users are unawares of pertinent privacy and security concerns facing them.

F. Consumers Mitigation

Process and policies adopted with the aim of minimizing data breaches and security incidents alongside the diminishing extent to which damage may occur is referred to as cyber security threat mitigation. But the pertinent question remains: what is the role of a consumer in mitigating data breach risk and thwarting hackers? There are various options designed at achieving mitigation function. These can range from simple low-level actions performed at a personal level, to organization-wide business strategy changes. It should be underlined that a number of simple practices and rules, when properly followed, can position individuals tasked with sensitive data at the required vantage point. This goes a long way in diminishing and preventing the degree of exposure to cybersecurity risks. Five categories of simple function designed for consumer mitigation exist: identify, protect, detect, respond, and recover.

When asked about the practices they take to secure their smart home devices, the practice of using a strong password to prevent unauthorized access ranked first, at 88.2%. The second practice is keeping data about devices safe and not sharing it with anyone outside the house, at 84.9%. The next practices are updating the IoT devices when the update is published and asked by device makers, as well as minimizing permission given to lower levels to access data, at 83.9% equally for each practice. The next practice is securing the Wi-Fi network inside the house and encrypting the data, at 82.1%. After that, making sure that all settings are properly and securely well configured, and working on the settings carefully with as few mistakes as possible, at 80.7%. Finally, asking and only buying the devices that consider security and privacy, ranked last, at 74.1%.

It should be underlined that every individual faces similar threats against organized attack, thus, every individual is

expected to protect all data and anticipate the worst possible attack scenario. Individuals who fail to regularly secure their software within the context of an IoT environment are likely to be attacked by sophisticated hackers. Previous practices would achieve cybersecurity goals in smart home devices.

There are three key primary goals of information security: (1) preventing the loss of availability, (2) the loss of integrity, and (3) the loss of confidentiality for data and systems. Most security controls and practices are designed to eliminate losses associated with each of the highlighted concerns. The aforementioned elements together form the AIC security triad. This represents the initials for availability, integrity, and confidentiality.

G. Stakeholders Responsibility

Given the fact that the risk factor has been clearly identified, has this helped in enlightening who should carry the responsibility of IoT security? Because of the many different participants in the operation and maintenance of security devices, there is a significant level of uncertainty. Guided by our research survey, 89.2% of the total respondents indicated that the one single body to bear this responsibility is the government, 74.6% indicated that consumers who are users of the devices are to carry this responsibility, and 74.1% placed the burden of responsibility on the manufacturers, as illustrated in Figure 6. All of these responses contain some degree of truth from the fact that each of these entities must bear responsibility, insofar as achieving a comprehensive IoT security is concerned. However, it is understandable that most respondents in the survey hold the position that governments should bear responsibility, being the main stakeholder of IoT security. Attaining this end requires that governments develop and implement policies and legislations aimed at monitoring and controlling the IoT market. This will serve to ensure compliance regarding the stipulated policies. In fact, the Ministry of Communication and Information Technology should use best practices and theory in IT as a way of strengthening the overall cybersecurity within the context of IoT.

Providers of IoT-enabled devices, such as manufacturers who are part of the security system, must effectively communicate and educate end users or integrators of any possible risk. By illustrating a commitment to protect users of their equipment, manufacturers are viewed as both understanding and trustworthy in the eyes of users. This can be attained by providing the necessary education to users. Another key and vital step that manufacturers can explore is encryption between devices, as a way of reinforcing protection within the IoT system. It is instructive that best protection with regard to data protection is developed whenever consumers use devices that are connected to a network. Some of the approaches of attaining this end are by disabling default credentials, practicing the safe sharing of sensitive information, use of proper and adequate password etiquette alongside the instinct to avoid any questionable requests or activities. Consequently, one of the best approaches of diminishing any misunderstanding regarding IoT security responsibilities is by roping in every contributor of the IoT enabled devices. Although concerns and fears regarding IoT are rife, a guarded and secure system can be attained by bringing together the manufacturer, the organization, and user.

H. Implication

Several security as well as privacy concerns have emerged because of the rapid and widespread adoption of technology. Moreover, the interconnectivity of the various different appliances has served to increase such issues. This comes at the backdrop of the fact that many users are oblivious to the dangers and risks of connecting their devices to their home network. It should be underlined that data generated and collected from smart devices can expose colossal volumes of personal information, for instance, likes, dislikes, and daily routines, thus revealing a lot about the user. Governments must take care of policies and legislation that protect users and preserve their privacy, while indicating the penalties for violating these regulations along with legislation to limit their abuse.

The United Kingdom also took the initiative of developing and publishing The Code of Practice for Consumer IoT Security, founded on 13 outcome-focused guidelines encompassing what is regarded as the generally acceptable tenets of good practice within the IoT security domain. In the same vein, the Canadian government has published a common understanding around the Internet of Things. This is highlighted as important in safeguarding the privacy of consumers within the IoT environment, as highlighted by the Internet of Things Security for Small and Medium Organizations.

However, as governments adopt such measures it should be acknowledged that individual users are expected to exploit best practices in addressing cyber perils as well as improving their levels of awareness by virtue of education.

Rating the security and privacy for each device that they purchased in the market is important to make other people aware and to notify vendors to pay attention to these issues. Vendors must provide transparency, including what data is being collected, in order to give the consumer the ability to control and manage their data with different options as well as to update the device to protect it when it faces an attack.

It is expected that organizations balance their need for connectivity and efficiency embedded in IoT technologies with risks and threats emanating from this connectivity. This is particularly the case given the prevailing absence of security-oriented design and development of these products.

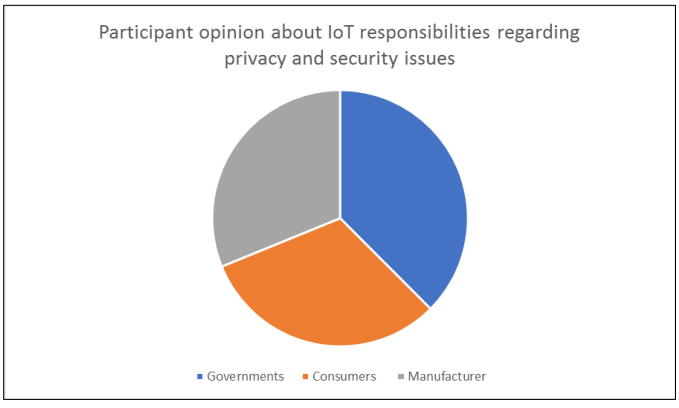

Fig. 6. Privacy and Security Responsibility Chart.

In order to prevent cybersecurity attacks within the context of the IoT environment, there is need to adopt a number of useful technical solutions by both consumers and vendors. This is informed by the reality that consumers are expected to create their layer of defense. One of these approaches is the use of multiple routers in order to be able to set up optional networks. Similarly, a router possesses the ability to separate different computing devices from IoT devices by directing them towards different numerous available networks. This makes it difficult for cyber criminals to attack effectively, because an attack on one device does not affect other devices on other different networks. To attain this end, consumers are required to check through reviews in order to get recommendations. Consequently, they are expected to perform research on security capabilities, buy or source their IoT devices from vendors and manufacturers with clear track records, and set automatic updates on their devices active for any available update.

VI. Conclusion

This research focuses mainly on the identification of all the security challenges that can arise because of the use of a large number of IOT devices connected to provide a smart home facility in Saudi Arabia. The beginning stage of the research focuses on the identification of the factors responsible for security concerns in smart homes. The research also tries to identify and provide various actions that can be taken in accordance with the problems associated with the protection of individual privacy and security against threats that might arise in the country. A realistic quantitative methodology is designed to identify the variety of people who are affected due to such security threats. However, it is really clear that, wherever data exists, there are probability and chances for concerns towards data stealing, breaching, hazards, etc. Therefore, the entire research is focused mainly on a large number of factors that are responsible for any security or privacy threat. Towards the conclusion of the model adapted in this research, benchmarking results are expected to be obtained and analyzed for the minimization of problems associated with security and privacy threats in Saudi Arabia.

References

[1] Weiser, M. Ubiquitous computing. in ACM Conference on Computer Science. 1994.

[2] Khan, Y. 5 Essential Components of an IoT Ecosystem. [English] 2020 21 April 2020 [cited 2020 21 April]; Available from: https://learn.g2.com/iot-ecosystem.

[3] Sato, H., et al. Establishing trust in the emerging era of IoT. in 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE). 2016. IEEE.

[4] Program, Y.E.-G. The National Strategy for Digital Transformation in Saudi Arabia. Digital Transformation [English and Arabic] 2020 24/11/2020 2020]; 1:[GOV.SA]. Available from: https://www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation/!ut/p/z0/04_Sj9CPyksy0xPLMnMz0vMAfIjo8zivQIsTAwdDQz9LUxNnA0Cg11DXEydAowCHQ31g1Pz9AuyHRUB1eTRhg!!/.

[5] Aleisa, N. and K. Renaud, Yes, I know this IoT device might invade my privacy, but I love it anyway! A study of Saudi Arabian perceptions. 2017.

[6] Fabi, V., G. Spigliantini, and S.P.J.E.P. Corgnati, Insights on smart home concept and occupants' interaction with building controls. 2017. 111: p. 759-769.

[7] © Maevi Sdn Bhd | 2017 -2020, A.R.R. The History Of Smart Homes. The Beginning of Home Automation 2020 [cited 2020; Available from: https://maevi.my/the-history-of-smart-homes/#:~:text=In%201966%20%E2%80%93%201967%20%E2%80%93%20ECHO%20IV,turn%20appliances%20on%20and%20off.

[8] Emeakaroha, A., et al., A persuasive feedback support system for energy conservation and carbon emission reduction in campus residential buildings. 2014. 82: p. 719-732.

[9] Nilsson, A., et al., Smart homes, home energy management systems and real-time feedback: Lessons for influencing household energy consumption from a Swedish field study. 2018. 179: p. 15-25.

[10] Heartfield, R., et al., A taxonomy of cyber-physical threats and impact in the smart home. 2018. 78: p. 398-428.

[11] Ferrag, M.A., et al. Privacy-preserving schemes for fog-based iot applications: Threat models, solutions, and challenges. in 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT). 2018. IEEE.

[12] Wang, Z. Personal information security risks and legal prevention from the perspective of network security. in The International Conference on Cyber Security Intelligence and Analytics. 2020. Springer.

[13] Lopatovska, I.J.U.J.o.L. and I. Science, Overview of the Intelligent Personal Assistants. 2019. 3: p. 72.

[14] Hall, F., et al., Smart Homes: Security Challenges and Privacy Concerns. 2020.

[15] Oltermann, P.J.T.G., German parents told to destroy doll that can spy on children. 2017.

[16] Atlam, H.F. and G.B. Wills, IoT security, privacy, safety and ethics, in Digital Twin Technologies and Smart Cities. 2020, Springer. p. 123-149.

[17] Sivaraman, V., et al., Smart IoT devices in the home: Security and privacy implications. 2018. 37(2): p. 71-79.

[18] Abraham, E.A.J.A. and I. Research, The Challenges Of Security In Internet of Things (IoT). 2019. 6(3): p. 165.

[19] Lim, H.-K., et al., Federated reinforcement learning for training control policies on multiple IoT devices. 2020. 20(5): p. 1359.

[20] CITC, K. Quality Of Service Indicators 2020. 2020; Available from: https://www.citc.gov.sa/en/Pages/default.aspx.

[21] Alanazi, M.H. and B. Soh, Investigating cyber readiness for IoT adoption in Saudi Arabia. 2020.

[22] Plachkinova, M. and P.J.I.S.F. Menard, An Examination of Gain-and Loss-Framed Messaging on Smart Home Security Training Programs. 2019: p. 1-22.

[23] Alam, T., et al., Big Data for Smart Cities: A Case Study of NEOM City, Saudi Arabia, in Smart Cities: A Data Analytics Perspective. 2021, Springer. p. 215-230.

[24] IOT, S. Annual Saudi IOT Conference. 2018 [cited 2018; Available from: https://saudiiot.com/iot-conference/.

[25] SaudiGazette. Business In Saudi Arabia. 2020; Available from: https://saudigazette.com.sa/article/590331.

[26] Al-Khattaf, D.-I. Saudi Arabia's IoT Market to Exceed $3 Bln by 2023. 2020; Available from: https://english.aawsat.com/home/article/2659731/saudi-arabia%E2%80%99s-iot-market-exceed-3-bln-2023.

[27] Siegel, D.J.C.M., available at http://changingminds. org/explanations/needs/control. htm, The need for a sense of control. 2008.

[28] Weinstein, M.J.H.P., What your FitBit doesn't want you to know. 2015.

[29] CITC, K. Regulatory materials on cloud computing:. 2021 [cited 2021; Available from: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx.

[30] Cekerevac, Z., et al., Internet of things and the man-in-the-middle attacks–security and economic risks. 2017. 5(2): p. 15-25.