The Cyber Security Risks of Using Internet of Things (IoT) Within the Domiciliary Care Sector

Abstract—**This paper considers the domiciliary care sector using the Internet of Things. Beginning with market research and industry analysis, it identifies the stakeholders and possible applications of IoT technologies and devices in home care for elderly people. Moreover, as IoT technology involves a great number of security risks, the paper also covers cybersecurity risks in home care automation, and an analysis of these risks was completed. Also, two surveys were conducted, one for end-users and another for home care providers, both providing vital insights and useful outcomes, which can be used to understand attitudes among the target audience. Also, the strategy for entering the IoT security market can be planned according to the results of this paper.**

Keywords— IoT, security, cybersecurity risks, healthcare,

I. Introduction

In recent decades, modern medicine has risen to an unattainable level. Artificial intelligence, wearable devices, and sensors are slowly becoming common tools in healthcare. Modern technologies are used for the diagnosis of diseases, treatment, monitoring, and operations. IoT devices for home care for the elderly are needed in order to control the heating in the house, give out medicines at the right time, monitor physical activity, and even initiate monitoring of the expiration date of products to prevent food poisoning. When planning an application of IoT it is essential to consider how to connect the devices and interact with them. In this way, it will be possible to determine which connection protocols apply to it. The required type of connection depends on the device, its functions, and its users. Typically, the distance over which data should be transmitted (short or long-range) determines the needed type of IoT connection. Short-range IoT network solutions are well suited for home, office, and other small environments. Small batteries are sufficient for their use, and sometimes they can be configured without using a battery. As a rule, they are quite economical in operation. Bluetooth (+Bluetooth Low-Energy (BLE)), Radio Frequency Identification (RFID), Z-wave, and Zigbee are examples of short-range IoT network solutions. Long-range IoT network solutions provide communication at 500 meters and more. They are characterized by minimal power consumption and are used for most IoT devices. For example, Low-power Wide-area Network (LoRaWAN) provides connectivity between mobile bi-directional secured devices which are powered by the battery. Cellular (3G/4G/5G), 5G IoT networks, Cat-0, Cat-1, LTE Cat-M1, Narrowband IoT (NB-IoT), and Sigfox are examples of long-range IoT network solutions [1].

Nowadays there are both public and private IoT initiatives in the home care segment for elderly people. The infrastructure of these services is based on providing remote access to medical services for people with health problems, especially for elderly people. Using a combination of equipment and technology, these services allow healthcare providers to monitor their health, manage treatment or diagnose painful conditions without the need for surgery or calling a doctor at home. devices monitor the health condition of the observed user (heart rate, blood pressure, body weight, or blood sugar) remotely through a computer unit connected to the Internet in the house, after sending all the data to the data center. The testimony is passed on to the medical professional in the clinic, who decides whether the intervention is necessary or not. To communicate with the monitoring center, landline telephone technology or an Internet connection is used.

The Internet of Things is expected to play an important role in health and medicine in the next few years. Thus, IoT systems contain private and vital information such as personal health care data. Smart devices may be connected to global data networks for access anytime, anywhere. Thus, IoT systems, even in the IoT healthcare sector, may be the target of attackers. Identifying and analyzing IoT security and privacy is critical to the full acceptance of the Internet of Things in the field of healthcare [2].

This paper is organized as follows. In Section II, cybersecurity risks in home care automation and analysis of these risks were completed. In section III, two surveys were conducted, one for end-users and another for home care providers. Finally, the paper is concluded in section IV.

II. Risk Analysis

Cybersecurity is very dangerous as it can cause serious damage. The impact varies from physical failure and shut down of important devices, the disruption of networks, and the theft of valuable data. Common cybersecurity issues with IoTs are as follow [3][4]: Easily cracked passwords: most passwords are easily guessed. This included unauthorized access through backdoors in firmware. Weak network services: for performance optimization network security is often neglected. Significant loopholes and vulnerabilities can be exploited. Insecure interfaces: whether it is a web, mobile, or cloud. It is considered a vulnerability because of the lack of appropriate security mechanisms; it is also hard to control access to these portals. Insecure update mechanisms: this includes patches and updates that can cause damage to the system; secure support after sales is not always guaranteed. Insecure component: some devices use outdated or optimized software or OS as well as well as untested technologies. These threats can also come from unverified third-party sellers. Lack of appropriate privacy protection: users' personal data stored in the device can be used without permission and dangerously. Insecure data transfer, processing, and storage: this is due to the weak or absence of adequate encryption, control access. Lack of device management: device management is critical to ensure device functionality as well as its security. it covers the process of authentication, provisioning, configuration, monitoring, and software/firmware maintenance. Insecure default setting: some device comes with weak security settings and restricts users from making any changes. Lack of physical hardening: malicious third parties can get hold of the device during the supply chain extract sensitive device details and even rig the device.

To identify risks on home automation technologies, IoTs, patients, and home care providers, we used risk analysis. The goal of this analysis, in this case, is to quantify risk in terms of the impact it causes to those assets.

Risk = Impact × Likelihood

Likelihood=frequency×probability of a breach/vulnerability's exploitation

Risk analysis Steps:

- Identify assets to be protected
- Identify vulnerabilities
- Identify threats (DREAD model)
- Risk Evaluation

A. Security Vulnerabilities

Cyber security attacks can be the results of unsecured vulnerability. Attackers exploit vulnerabilities in systems to launch an attack. Examples of vulnerabilities include:

- Commonly used systems in IoT for supervision or data acquisition and treatment. This includes Windows-based PC, SQL servers, and archival services
- Commonly used networking technologies (Ethernet and TCP/IP...etc)
- Poorly designed security systems embedded systems in IoT
- Outsourced development of critical software in IoT that can be accessed, sold, or hacked elsewhere.
- Other vulnerabilities include Software vulnerability, Networks vulnerability, and Hardware and device vulnerability.

Major operating systems (OSs) are the main reason behind device attacks. Many devices are based on Microsoft Windows or Linux. Attackers understand very well those OS and their vulnerabilities. The industry lacks specific operating dedicated to IoTs that support security. Or simply, some private operating systems are designed to ensure performance and security are not looked at as a priority. One known security measure is the use of security patches. However, this requires that device providers using standard OSs and/or applications need to assure that the patches don't fix something and break something else. Usually, in similar industries, private companies and ssuppliers often do their own testing and issue their own patches. Patches keep systems security up to date against new threats. It is crucial to find the right suppliers who regularly provide software updates and security patches as many avoid doing it because they perceive it as an additional cost. System heterogeneity, this vulnerability is not tied to the software only but also includes the hardware. This applies to networking standards and software updates as well. Depending on the vendors, many devices come with little documentation about the device in terms of software/firmware operating systems, security. The credibility of the vendors is important. any certification and accreditation are good. Private suppliers who ensure a secure supply chain and full private development have better advantages. The vulnerability exists in TCP/IP library and it allows remote code execution which can be badly exploited to affect the device. 11 big IoT vendors have been identified as having this vulnerability. Networking standards used in home automation Different IoT in home automation use different networking standards depending on the supplier. These standards have their weakness and strength. Some home automation IoT use different standards which make it hard to secure. Application and messaging, likes, HTTP, XML, JSON, RESTFUL, MQTT, CoAP, XMPP, DDS. Network and transport, likes, IPV6, 6LoWPAN, RPL, TCP/UDP, TLS, DTLS, Aeron, ROLL. Physical Devices and Communication, likes, Zigbee, Bluetooth, Wi-Fi, 4G/5G, LTE, LTE, VSAT, LoRaWAN, NB-IoT, and Weightless are some of the standards and protocols [5].

Different messaging protocols have some vulnerabilities. These vulnerabilities can cause security risks due to lack of security service or incorrect configuration [6]. Some protocols don't have any security protocols like CoAP (no authentication and authorization mechanisms). SASL offers more configuration options which can lead to incorrect configuration. TLS and DTLS have a difference with Internet Protocol (IP) traffic. TLS uses TCP and DTLS uses UDP. UDP is less secure than TCP [7].

Wireless communication: IEEE 802.11 (wireless Ethernet) is one widely used. It has different security features like Wired Equivalency Protection WEP, Wi-Fi Protected Access/Wi-Fi Protected Access II WPA/WPA2, and 802.11i. WPA2 with AES encryption is recommended. WEP Encryption scheme has been hacked. One issue of wireless networks is that network radio transmissions extend over house boundaries. This fact makes the network available for outsiders. Hackers have shown that they contact access points 1°s from miles away using amplifies. As a policy, companies restrict employees from using devices in public areas. The reason behind this policy is similar to patients who have home automation. Portable devices that can move between areas like a laptop, the phone is a risk. Users can carry threats from insecure areas and bring them back to the secured network. Once infiltrated, the threat (e.g. virus) can run behind firewalls, spread to other systems, and disclose/transmit data. This can be done using ssimilarly infected portable devices like USBs, hard drives, CDs. Etc. That can be inserted into a computer are also a threat. When inserted, the auto-execute file will propagate through the whole system or make malicious activity. IoT computing devices are also known for their weak or not as powerful computing compared to other devices like laptops. This resulted in avoiding complex security yet effective security algorithms. IoT devices have limited memory, low energy, and low-end (8-bit) micro-controller. Attackers can take advantage of this to deplete the device from its resources [8]. Additionally, it is possible that a device has been rigged and physically opened. This can happen during the pre-deployment phase or in the development/manufacturing/packaging phases [9]. IoT and 5G are considered new technologies and to put it simply, current cybersecurity standards are not anticipatory enough for these technologies and they require better security. Vulnerability is still to be discovered and covered. Some of the vulnerabilities consist of:

- Hackable numerous smart devices are all connected to a network; some sensitive devices are connected like power supply and vital medical devices. Attacks affecting these devices will have a major impact [10].
- Bandwidth expansion in 5G;

- 5G network is managed by software. Losing control of the software puts the whole network at risk;
- Network functions are now virtualized in software compared to being done by physical appliances before; and
- The network is now distributed and software defined digital routing.

B. Methods of Attack

Attacks on home automation are not only about the devices. The attacks target internet users through different channels using conventional cybersecurity attacks. Social engineering is when the attacker unsuspectingly asks for information from the elderly victim for malicious reasons. The collected information can be used to enter a house, collect financial details or trick the user into unintentionally starting a cyber-attack. In order to access IoT devices and even the whole care system, attackers usually take advantage of different methods to interact with the elderly and trick them into taking action that will ease their infiltration into the system. An example of this would be a questionnaire for examples sent to the elderly asking them to answer specific questions related to equipment and configuration of the devices they have in the house. This information can be used later to tailor their attack to be more precise. Another attack can be by pretending to be one of the care providers to lose their access to WIFI, elderly account and ask for contact details or details that they can use to log on. Another widely used method is phishing. The elderly receives message or email telling them that they have been logged out of an account or payment hasn't been processed and asking them to redo it. This can be asking for bank details, PIN, or credit card. Other message contain a hyperlink to a web page that downloads malware. Common types of social engineering targeting the elderly comprise: Phishing, Spear phishing, Angler Phishing, Baiting, Malware (trojan horse, Scareware, ransomware, spyware...etc.), Vishing/Smishing, Honey trap. Internal threats can happen by a disgruntled employee who already has access to a system. An employee can sabotage files and devices, give a hacker access to the system by diffusing critical information or insert time bombs that initiate after he has already left whether to hurt the company's reputation or for other reasons. unhappy employees might hold a grudge toward a company or manager and sabotage a project or device. He can also see an opportunity to take advantage of the client/user. At the same time, Internal threats can be unintentional. In this case, it can result from both the employee and the user. It includes

- Issue with System
- Bad training may result in bad/incomplete installation.
- Bad training on security policies
- Improper use or improper curiosity of employees or the elderly
- The accident causes the device to malfunction, reset or stop working.

Password cracking issue relates to Poor password management. It affects both sides. One main issue with a strong password is the difficulty to remember it especially for the elderly. This leads the elderly to use other methods to store their passwords like writing them on a piece of paper which can be easily stolen. If the password is not strong enough it becomes easy to crack especially if they came with system default passwords. Other password cracking tools exist.

C. Risk evaluation

We put a list of possible consequences of a compromised system:

- Endangerment of health and safety
- Financial Damage
- Interruption of health monitoring and missing valuable information
- Theft of Data and personal information
- Violation of regulatory requirements and compliances
- Violation of privacy
- Damage to company reputation
- Degradation of the QoL

Damage Potential is rated according to the consequences it generates. The total score incorporates threat and consequences and define the impact.

The cyber security risks in home care automation vary across different aspects. It is important to understand that attacks generate from other sources than the IoT and then expand to the home automation network. One of the major threats comes from social engineering attacks. This is due to many reasons explained previously that exploit a vulnerability in elderlies. Educating and supervising elderlies use of technology becomes a necessity. Additionally, the quality of the IoT devices used makes a difference in preventing attacks. Ensuring a valid, secure supplier and supply chain is necessary. Finally, IoT, Home automation technology, and 5G are relatively new technologies. Running penetration tests on hardware, software, and network-level is recommended.

III. Attitudes Among The Stakeholders

According to the market research, there were 3 primarily stakeholders identified for smart home technology in the domiciliary care sector: smart technology suppliers, care home providers, and the government. The end-user (buyers) of the domiciliary care service were considered in order to obtain the full perspective of the attitudes of the target audiences of the industry. The instrument used for collecting the data was the survey and 2 versions were made. The first one is for the people who receive the domiciliary care service or the buyers (people who know that their relatives need the domiciliary care) and the second one was for the home care providers.

According to the survey's findings, there are 4 different types of consumers identified. The first is the individuals who do not require care, but a member of their family does (buyers). The second is the individuals over 56 that could require care (end-users). The third is the home care providers that are using any kind of IoT technology and the fourth is the home care providers who are not using IoT technology in their care services. Therefore, in order to analyze the results for all groups of consumers, a set of themes were established to examine and collect the data in broad patterns.

TABLE I: RANKING OF THE IMPORTANT FEATURES OF IOT IN THE DOMICILIARY CARE SECTOR

Aspect/rank	1	2	3	4	5	6	7	8
Cost	16.67% 26	8.97% 14	15.38% 24	17.31% 27	10..26% 16	8.33% 13	10.26% 16	12.82% 20
Qualiti of care	42.31% 66	22.44% 35	14.74% 23	8.97% 14	3.85% 6	4.49% 7	1.28% 2	1.92% 3
Convenience for you and your family member	7.05% 11	12.82% 20	17.31% 27	16.03% 25	18.59% 29	13.46% 21	10.26% 16	4.49% 7
Installation of devices and systems	1.28% 2	1.92% 3	5.77% 9	7.69% 12	13.46% 21	14.10% 22	22.44% 35	33.33% 52
Functional competence	2.56% 4	9.62% 15	6.41% 10	10.26% 16	11.54% 18	21.79% 34	25.00% 39	12.82% 20
Patien comfort	14.74% 23	21.79% 34	15.38% 24	12.18% 19	12.82% 20	10.90% 17	7.69% 12	4.49% 7
Security	8.97% 14	10.90% 17	13.46% 21	15.38% 24	14.74% 23	15.38% 24	15.38% 24	5.77% 9
Privacy	6.45% 10	11.61% 18	11.61% 18	12.26% 19	14.84% .23	11.61% 18	7.74% 12	23.87% 37

A. *end-users analysis*

The first analysis is related to the buyer's survey. In which the main objective is to identify if there is a potential market for IoT domiciliary care. The results show that 57.05% of the respondents said that if they have the opportunity to choose, they are willing to use the domiciliary care supported by IoT. Despite the lack of understanding of the Internet of Things, since only 31,82% of the respondents understand completely the meaning of the Internet of Things related to home care. However, this pattern extends further to one of the groups of consumers. Since 3.25% of the respondents over 56 years understand fully the meaning of this technology. Nevertheless, this doesn't affect the decision for them to implement IoT in their homes considering that 7.14% prefer to have it compared to the 2.60% that would prefer regular domiciliary care. This means that the majority of end-users interviewed in the survey are willing to receive domiciliary care services supported by IoT than the regular domiciliary care that the home care companies provide. Of the remaining 89.61% of respondents (those under 56), 49.35% prefer domiciliary care supported by IoT for their relatives while the other 40.26% prefer regular domiciliary care. The gap between the buyers that prefer regular domiciliary care is not that big. Therefore, it is necessary to address the reasons why that high percentage prefer regular domiciliary care in order to contrast them with the security and privacy concerns that are believed to be the reasons why they are reluctant to implement this technology in their homes as it is stated in the first hypothesis of the survey.

the reasons behind the percentage of the respondents (40.26%) prefer regular domiciliary care is because of privacy and security concerns. Given that those 2 reasons have a major impact when it comes to deciding which type of domiciliary care they prefer. Since each one of them cover 25.20% respectively. Followed by cost with 16.54%, ethical concerns with 13.39%, lack of IoT with 12.60%, and other reasons with 7.09%. These findings support the first assumption that was made in order to identify the reasons why people are disinclined to adopt new technologies in their homes. In addition, the respondents were asked to rank the most important features for them if they were offered domiciliary care supported by IoT. The quality of care and patient comfort are the factors that are most significant if they are going to use IoT domiciliary care services. The least relevant factor is the installation of devices and systems. It indicates that the patient's wellbeing is the most important aspect regardless of the different types of domiciliary care services they receive. Leaving the security and privacy concerns on a different level of importance when it comes to comparing with the patient welfare. For further information see Table I. Moreover, in order to perceive the awareness of the cybersecurity risks inherent to the implementation and usage of the IoT system and devices, a list of risks was displayed to the respondents. At least one person had never heard of each of the 10 cybersecurity risks presented. The more unusual risks (ones which they had never heard of) from the respondents' perspective are: Denial of service (16.15), Pretexting (social engineering) with 14.84%, Baiting (14.32%), Vishing (10.68%), and key logging programs (10.16%). On the other hand, the risks that they have a strong understanding of are: Phishing emails (17.03%), Password cracking (12.66%), Smishing (12.66%), and Malware (11.79%). 78.21% of the respondents believe that the potential of these risks directly impacts the decision of using IoT domiciliary care. Being 71.06% of that percentage from buyers (under 56) and the 7.14% remaining from end-users (over 56). This implies that there is a market opportunity for domiciliary care services supported by the Internet of Things if the patient's welfare and comfort are considered a priority and the security and privacy issues of the IoT systems are explained in detail. In order to enhance the awareness of the cybersecurity risks and their ways to prevent them with the aim to increase the willingness of using this technology in the domiciliary care sector.

B. *Home Care providers analysis*

The second analysis is of the home care providers. A survey was conducted among 15 home care companies all over the UK. In order to determine if they are adopting any kind of technology and their awareness of the cybersecurity risks associated with IoT systems and devices. The results from this survey reveal that there are 2 types of providers: the home care providers that are using IoT and the home care providers that are not using IoT. Therefore, the analysis in this part is going to be divided into these 2 groups since different questions were asked according to if they are currently using IoT or not. The findings show that 66.67% of the respondents offer some form of smart home technology to support their care services. 36% offer smart sensors systems such as: door, seat, tap, shower, bed, and plug with their care services. Following this is wearable devices with 28%, smart home devices (speakers, light bulbs, medication reminders) with 16%, 12% for health monitoring systems that track the heart rate, blood pressure, and temperature, and 8% for location tracking systems such as GPS.

Additionally, the primary security concern that they have regarding the implementation of technology is the exposure of the patients' personal details and media (14.58%) followed by the data being used by third parties for undisclosed reasons (10.50%), the company or the patients being exploited by malicious attackers, the negative reflection of the company if a hack event occurs, encountering malicious files, taking advantage of by other companies and malfunction of the device all come in at 10.42%. For further information see Fig. 1. In contrast, 33.33% of the fifteen care companies surveyed are not using any form of technology in their care services. However, the survey shows that they are looking to implement smart home devices and smart sensor systems with 27.27% of respondents wanting to introduce these technologies, followed by wearable devices with a percentage of 18.18%. Despite that, 18.18% chose that they don’t want to implement any kind of IoT devices. Hence, the decision to identify the reasons for not adopting this technology to support their care services. The main reason being cost at 27.27%, followed by the lack of infrastructure with 18.18% and other reasons (18.18%) such as “we provide domiciliary care, therefore sensors in customers’ homes need to be arranged with customer/family directly” or “understanding of the age group we work with” these are direct quotes from the care companies that answered the survey. Leaving privacy issues with a 9.09% response rate and the security issues with no percentage at all. To see more information about the answers, check Fig. 2. Moreover, they were asked about which security concerns they would have if they decide to implement technology into their care services. The biggest issue is the loss of devices with 28.31%, followed by the malfunction of the device that can cause harm to the patients with 14.29% and the patient’s identity being stolen with the same percentage. From the 15 home care companies 22.22% of them believe there will be a strong positive impact on security for patients and companies following implementation of IoT into their care services and they also believe that the well-being of the patients will be strongly positively impacted with 22.22% of respondents choosing this option. This shows that the reasons why the buyers and end-users are reluctant to adopt this technology (security and privacy) are the same factors the care companies think will benefit from using IoT in their care service (somewhat paradoxically). Therefore, based on the thinking of the care companies regarding these 2 issues of the buyers and end-users. There is a clear connection between what the market wants and what the care companies are willing to offer to their patients, in terms of security and patients’ well-being. On top of that, in order to determine their understanding of the cybersecurity risks, 15 different risks were displayed such as: malware, denial of service, phishing emails, baiting, smishing, vishing, pretexting (social engineering), key logging programs, password cracking, data breached, network attacks, virus, trojan horse, ransomware and spyware. The most uncommon (ones which they had never heard of) being, pretexting (27.27%) and vishing (13.64%) and the ones that they have a strong understanding: phishing emails (11.11%) and viruses (11.11%). However, it is important to highlight that every risk presented had at least one company stating they had a full understanding of them, whereas some risks were never chosen to be completely unheard of (e.g. no company chose the ¸option of complete lack of understanding for´malware´and´virus´).

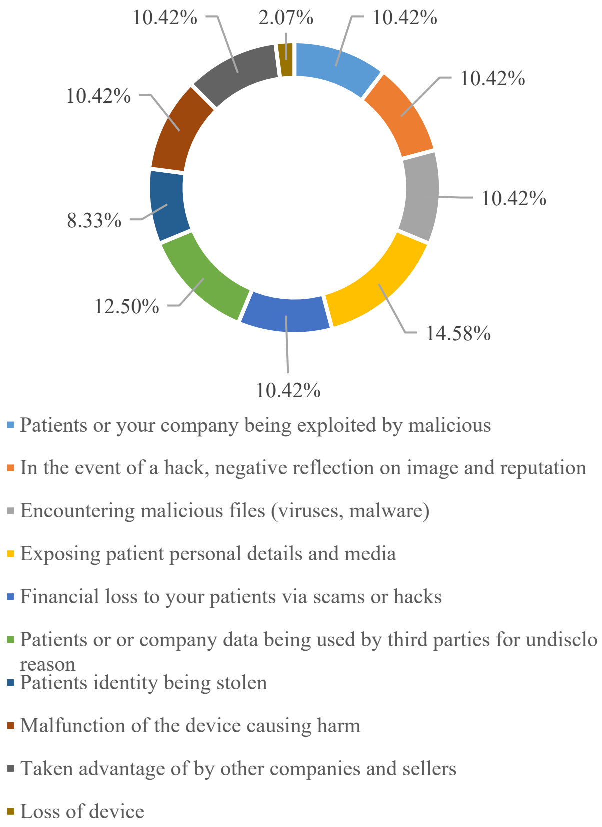

Fig 1. Security concerns towards the implementation of IoT in domiciliary care of the Home Care Providers using IoT.

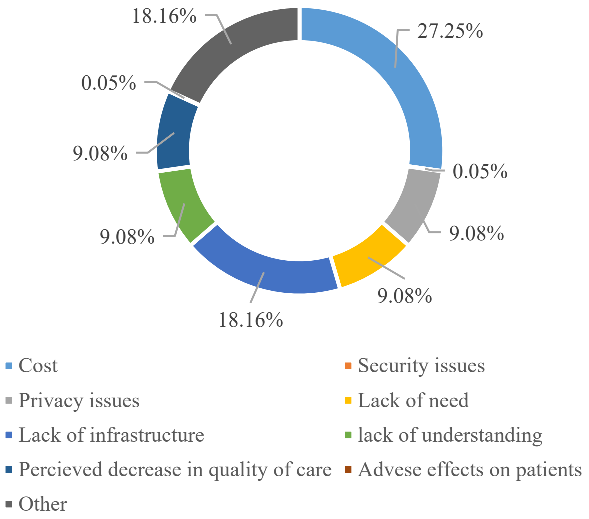

Fig 1. Reasons for not adopting IoT in domiciliary care sector.

At the same time, 60% of the home care companies believe that their patients are inclined to be targeted by the cybersecurity risks To conclude the analysis the providers were asked to share their views and opinions on the adoption and use of IoT in the domiciliary care sector in an open question. Their responses include insightful and meaningful information on the thinking of homecare providers when it comes to the adoption of IoT that cannot so easily be gained by looking at the percentage responses to closed questions.

C. Secondary research: elderly people

As the elderly end-users of the systems were not surveyed, it is important to look at existing research on their attitude towards the adoption of technology and their willingness to do so. Much research exists on the subject and the following is a summary of the most important findings that are relevant to this case. the most definitive and useful research available on this topic is [11], which concludes that eight factors impact the elderly's willingness to adopt healthcare technology. These are: performance expectancy (the benefits and performance the technology can offer), effort expectancy (the effort required by the user to gain benefits), social influence (other people's views on the technology and its benefits/negatives), facilitating conditions (the organization and infrastructure available in support of the technology), technology anxiety (the anxiety felt from the use or expected use of the technology), perceived trust (security and privacy of the technology), perceived cost and finally expert advice (the advice available from experts in relation to the benefits and use of the technology). Previous studies had always identified performance expectancy as the most important factor, however, [11] conclude that actually effort expectancy is most important in influencing the elderlies' decision to adopt technology as this effort is viewed in relation to the expected benefits of the technology and then the decision to adopt or not is based upon whether the elderly individual views the effort as worth it. However, despite this, their findings place all eight factors as all holding significant weight in the decision-making process.

IV. Conclusion

While using smart gadgets and information systems promises better life quality, easy to access services and connect individuals with their support network, it seems that the magnitude of deployment challenges and potential adverse impact are still not fully known. The study presented in this paper shows that there is yet a moderate appreciation for the types of cyber security threats to the dormitory house when they implement assistive modern technologies like health IoTs. That said, care takers are worried abut their personal details being exposed and clearly highlighted the importance of securing their personal information. Similarly, care providers are also concerned with the cost of technology infrastructure and it is use potential impact on information security and privacy. For future work, we would like to 1) understand the effective use of using health IoTs in dormitory houses then, 2) propose a methodology and framework for secure use of health IoTs that covers aspects of end-users, devices, data transmission, storages and infrastructure.

References

[1] S. Al-Sarawi, M. Anbar, K. Alieyan and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," *2017 8th International Conference on Information Technology (ICIT)*, 2017, pp. 685-690, doi: 10.1109/ICITECH.2017.8079928.

[2] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[3] M. Abomhara, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65-88, 2015.

[4] N. Miloslavskaya, et al. "Standardization Issues for the Internet of Things." *World Conference on Information Systems and Technologies*. Springer, Cham, 2019.

[5] M. A. Khan and K. Salah, ''IoT security: Review, blockchain solutions, and open challenges,'' *Future Gener. Comput. Syst*., vol. 82, pp. 395–411, May 2018.

[6] G. Nebbione and M. C. Calzarossa, "Security of iot application layer protocols: Challenges and findings,"*Future Internet*, vol. 12, no. 3, 2020.

[7] M. Friesen, G. Karthikeyan, S. Heiss, L. Wisniewski, and H. Trsek, "A comparative evaluation of security mechanisms in DDS, TLS and DTLS," *Kommunikation und Bildverarbeitung in der Automation*. Berlin, Germany: Springer-Verlag, 2020, pp. 201–216.

[8] Lin, H., and Bergmann, N. W., "IoT privacy and security challenges for smart home environments". *Information*. 7(3), 2016

[9] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 163-168, doi: 10.1109/TrustCom/BigDataSE.2018.00034

[10] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682-3722, Fourth quarter 2019, doi: 10.1109/COMST.2019.2916180.

[11] D. Pal, S. Funilkul, N. Charoenkitkarn, and P. Kanthamanon, "Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective," *IEEE Access*, vol. 6, pp. 10483-10496, 2018, doi: 10.1109/ACCESS.2018.2808472.