Home Care Automation: Market Research, Industry Analysis, and Security Assessment

Amjad Fayoumi
Management Science
Lancaster University
Lancaster, UK
A.Fayoumi@lancaster.ac.uk

Somayeh Sobati-Moghadam
Department of Computer Engineering
Hakim Sabzevari University
Sabzevar, Iran
S.Sobati@hsu.ac.ir

Abolfazl Rajaiyan
Electrical Engineering Department
Ferdowsi University of Mashhad
Mashhad, Iran
A.Rajaiyan@mail.um.ac.ir

Charlie Oxley
Management Science
Lancaster University
Lancaster, UK
c.oxley@lancaster.ac.uk

Paula Florez Montero
Management Science
Lancaster University
Lancaster, UK
p.florezmontero@lancaster.ac.uk

Artur Safarian
Management Science
Lancaster University
Lancaster, UK
a.safarian@lancaster.ac.uk

***Abstract*— Due to the low availability of carers worldwide, technological means to meet the ever-increasing demand for care services are increasingly necessary. This paper discusses how the IoT is being used in the domiciliary care sector in the UK. It begins with market research and industry analysis to identify stakeholders and the possible application of IoT technology and devices in home care for elderly people. Since IoT technology is inherently vulnerable to security threats, the paper discusses security in home care automation, and also conducts a risk evaluation. This analysis and evaluation can be used to learn more about the target audience's mindset. The results of this research can motivate and inform technology companies to enter the IoT market.**

***Keywords*— Internet of Things (IoT), market research, IoT security, care home, digital healthcare.**

I. Introduction

The IoT is an important emergent technology that has numerous applications in various fields. One vital field in which the IoT can be used is the healthcare sector. Applications of IoT in the healthcare sector promise to enable timely and excellent provision of medical services to patients through remote assistance. Many medical applications, such as fitness programs, e-personal assistants, health monitoring devices, and remote monitoring of health and home remedies are offered using several mobile and ubiquitous applications. There are several IoT healthcare technologies, such as Radio Frequency Identification (RFID), edge computing, semantics technologies for natural language processing (NLP), cloud computing, Big Data, grid computing, Augmented Reality (AR), and actuators [1]. In the last decade, many research articles have presented architectures, applications, and scenarios for IoT in healthcare, including IoT solutions for diabetics, and non-invasive respiratory monitoring systems to automatically control ketoacidosis symptoms [2]. The experiment results showed that innovative development produced reliable outcomes. Another application of IoT in healthcare is related to home care for elderly people.

IoT for home care for the elderly is seen as a highly desired alternative option that allows for extensive monitoring of various symptoms and conditions of elderly residents and their dwellings, while also offering a sense of freedom for the observed person. Despite the risks of ageing, the elderly generally want to live autonomously and independently to the greatest extent possible. These aspirations provide additional challenges in assisting the elderly with safety and risk monitoring, particularly when using technology. Living alone might lead to no one being able to react in time if an emergency scenario arises. Patients' lives, as well as the quality of services provided by healthcare professionals and the government, could benefit from the use of healthcare IoT.

As technologies advance and their use increases, the challenge of security and data privacy should be investigated in greater depth. IoT technologies transmit sensitive data, and hackers are constantly targeting IoT devices, as they are vulnerable in their nature due to the volume of data they collect and (potentially) transmit, which can be used for nefarious purposes (e.g., in ransomware attacks, or for sale on the Dark Web). Due to elderly people generally lacking awareness of emerging technologies and how to handle security threats, it is important to examine the security of IoT systems used in elderly care [3-4]. Several research studies introduced developments to increase the security of IoT-based systems, such as Wireless Body Area Networks (WBAN) anonymous authentication, which has proven to be secure [5].

The remainder of this paper is organized as follows. Related works are reviewed in section II. Section III analyses health IoT market research, and section IV identifies key stakeholders and their requirements for smart technology in the domiciliary care sector. Section V explores and evaluates security in home care automation, and the paper is concluded in section VI.

II. Related Works

Due to the increasing use of the IoT, various deployment and adoption challenges have emerged, and current studies are increasingly focused on adoption implications [6-7]. Because of the convenience they provide to homeowners, IoT-based smart home systems are becoming increasingly popular among modern IoT applications. The designs and applications of such systems should consider the effects of power consumption, security, market readiness, user sentiment, and the efficiency and effectiveness of the deployed systems themselves. Several recent studies have addressed these issues, including extensive research to improve the performance of IoT-based systems.

One study developed a formula for developing IoT-based systems based on available power consumption, to optimize the power consumption of IoT-based systems [8]. Other

researchers designed high-speed IoT systems for use in applications where decision-making speed in near real-time is critically important [9], where high accuracy is a major priority [10-11]. Elkahlout et al. [12] reviewed previous studies on the development and application of IoT healthcare systems for the elderly, and included a description of the fundamental structure of IoT healthcare systems, as well as ways for implementing them in hospitals and at home. Tawalbeh et al. [13] investigated the methodology, applications, and tools of Big Data Analytics (BDA) and mobile cloud computing to explore their potential and importance in healthcare. Another study investigated concepts, uses, and numerous existent technologies in the healthcare sector, identifying differences between strategies for IoT deployment in healthcare [14].

According to a recent research study [15], consumer-perceived security rankings can now be created in a new way. The study examined previous attempts to use the Analytic Hierarchy Process (AHP) to prioritize security concerns. The proposed method can be implemented with any data from a security assessment study. The paper also provided a full examination of the security risks of devices utilized in smart homes when viewed through the lens of the IoT. Arif et al. [16] examined the security of smart homes in terms of the usage of blockchain technology, and investigated some existing smart home schemes that employ it. Bhuiyan et al. [1] surveyed improvements in IoT-based healthcare solutions and discussed state-of-the-art technology for an existing IoT-based healthcare system, and offered an overview of all potential digital-health based networks. IoT healthcare processes were reviewed in this framework, and a comprehensive discussion of their strengths and weaknesses was presented. Some of the weaknesses are related to technology capacity, cost, security and maintenance. Marshal et al. [17] analyzed security concerns that smart health devices face, and the required actions in order to improve security. Karunarathne et al. [18] examined the current condition of privacy and security in the healthcare sector, as well as the challenges associated with creating security frameworks, resulting in recommendations for effective privacy and security solutions. The security problems raised by IoT devices that require remote access to sensitive data were examined in this paper.

Based on our review, we suggest that further understanding from a market perspective is needed. Consequently, this study undertakes market research and industry analysis, identifying key stakeholders and potential applications of IoT technologies and devices in home care for the elderly, and discusses security in home care automation.

III. Market Research

A. Industry analysis: Home care sector in the UK

In 2020 the domiciliary care sector in the UK was worth an estimated USD 5bn, with 11,338 businesses operating within it employing 312,696 people. The average industry growth between 2015 and 2020 was 2.8% per year [19]. There are 350,000 elderly and 76,300 younger people with learning or physical disabilities or mental health challenges requiring home care within the UK [20]. The number of elderlies is expected to rise to 468,000 by 2035, and by 2024 the number of over 65's is expected to comprise over 20% of the population, resulting in more over 65's than under 15's. At any one time, there are up to 110,000 vacancies for staff within the sector, and the public authorities commission over 249 million hours of home care a year. This represents 76% of home care revenue, with the remaining 24% being met by self-funded private payments. The percentage coming from these private payments is set to increase by 49% to account for 36% of total revenue by 2035. A lack of privacy, high costs, perceived simplicity of use, and extensibility all have an influence on the adoption of existing home care safety and risk monitoring solutions.

B. Major domiciliary care providers

A look at the top 20 domiciliary care providers in every region of the UK (as well as the top 20 national providers) quickly shows that only a small fraction of the biggest and best providers are currently utilizing any substantial smart technology system to support their care services. This trend is also seen when assessing the domiciliary care providers advertised on the NHS website [21]. Table I shows the percentage of providers in each region (and nationally), ranking the top 20 that mention any form of IoT or smart technology in their offered care services. As shown, the percentages everywhere range from very low to moderate. However, the reality is much shoddier, as within the top 20 a singular care company (Home Instead Senior Care) accounts for every single provider utilizing IoT (they have multiple branches within the top 20 of each region). Not one of the other companies mention IoT/smart technology as a form of service they offer. It could be because the main focus of advertising is providing a caring and supportive atmosphere

TABLE I: MAJOR DOMICILIARY CARE PROVIDERS IN THE UK

Region	Total Companies	Companies Using IoT	Percentage
London	20	3	15%
East of England	20	2	10%
East Midlands	20	3	15%
North East	20	5	25%
South West	20	5	25%
South East	20	7	35%
West Midlands	20	7	35%
Yorkshire and The Humber	20	5	25%
Scotland	10	5	50%
Wales	20	3	25%
North West	20	3	15%
National Home Care Groups	20	1	5%
NHS Website	20	2	8.7%

IV. Stakeholders

Market research identified the following stakeholders for smart technology in the domiciliary care sector:

A. Smart technology suppliers in the domiciliary care sector
B. Home care providers
C. Government institutions

A. Smart technology suppliers in the domiciliary care sector

The first stakeholders identified are the producers and suppliers of the IoT devices used within the domiciliary care sector. Four identified within the UK were: Anthropos Digital Care, Tunstall Healthcare UK, Essence, and Karantis 360. Develco Products was also found, which is a Danish company that supplies the UK market.

TABLE II: ASSETS IN HOME CARE AUTOMATION

For the Elderly		For Care Providers	
Tangible & Financials	Intangible	Tangible & Financials	Intangible
• House & property • Cash • Credit cards • Bank and financial account details (e.g., retirement/ savings account) • Land/ house papers • Equipment (electronics and IoTs) • Personal documents • Vehicles • Valuable items	• Identity • Online activity data • Health data • Personal life details and activities • QoL domains: enjoyment, relationships, comfort, meaningful activities, security, functional competence, privacy, autonomy, spiritual well-being, and dignity	• IoT devices • Equipment • Company details • Employee information (credentials, salary, etc.)	• Computer programs • Patients database • Medical charts and records • Provider's brand name • Reputation • Supplier contracts

TABLE III: MAIN SECURITY OF MESSAGING PROTOCOLS

Protocol	Authentication		Authorization	Confidentiality		Possible Attacks
	SASL	Custom	Custom	TLS	DTLS	
Message Queuing Telemetry Transport (MQTT)		×		×		DoS/DDoS, MiTM
Constrained Application Protocol (CoAP)					×	IP Spoofing, DoS/DDoS, MiTM
Advanced Message Queuing Protocol (AMQP)	×			×		DoS/DDoS
Data Distribution Service (DDS)		×	×	×	×	DoS/DDoS
Extensible Messaging and Presence Protocol (XMMP)	×		×	×		DoS/DDoS, MiTM

Between them, these companies supply all possible IoT devices that may be required to establish an IoT-supported home care systems, including alarms, fall detectors, monitoring devices, smart hubs, sensors, and communication devices.

B. Home care providers

The providers of domiciliary care using IoT technology to support their care services are the second set of stakeholders. Four were identified within the UK: Home Instead Senior Care, from the top 20 home care provider awards; Allied Healthcare and The Good Care Group, from the list of home care providers advertised by the NHS; and Kingsley Home Care, from independent research. The specific systems they are all using are slightly differ from one another, but they commonly use wearable IoT devices to measure health vitals, and some form of sensors placed around the home to measure and/or detect various activities by patients. Other forms of IoT technology were also used, but not universally, such as communication devices, fall detectors, different forms of sensors (such as tap, door, bed, plug, and shower), and medication reminders.

C. Government institutions

The final identified stakeholder is governmental bodies. The adult social care system faces challenges in relation to the needs and demands of the market, the eligibility of the patients who need domiciliary care, funding, market sustainability and fairness, workforce and caregivers, quality and efficiency, and integration with the housing, health, and benefits systems. The

most important challenges pertain to workforce and caregivers, and service quality and efficiency, as these challenges result in high vacancy rates in a sector that needs to recruit increasing numbers of workers to meet demands, along with low investment in technology and new models of working to improve the quality of care. It is these challenges that result in the government becoming a key stakeholder for smart technology in the domiciliary sector. In response to the rising difficulties they face, government institutions produced an industrial strategy report, which makes improving the well-being of the ageing society a key priority, which is something that going to improve home care by using IoT[1]. Furthermore, the government also announced GBP 300 million to help tackle the 'landmark ageing society grand challenge', of which GBP 98 million is specifically to be invested in the 'healthy ageing program', which will drive the development of new products and services which will help people to live in their homes for longer, tackle loneliness, and increase independence and wellbeing.

TABLE IV: RISK EVALUATION AND SCORING

Threats	D	R	E	A	D	Total	Impact Level	Likelihood Score	Likelihood Region	Region
Social Engineering	2	3	3	3	2	13	H	6	H	HxH
Internal Threat	2	2	2	2	2	10	M	4	M	MxM
Password Cracking	2	2	1	1	1	7	L	2	L	LxL
Jamming Attacks	1	3	2	1	2	9	M	6	H	MxH
Low-level Sybil	1	2	2	2	2	9	M	4	M	MxM
Spoofing Attacks	1	3	2	2	2	10	M	6	H	MxH
Insecure Physical Interface	1	1	2	1	2	7	L	2	L	LxL
Sleep Deprivation Attack	1	2	2	1	2	8	M	4	M	MxM
Replay or Duplication Attacks Due to Fragmentation	2	2	2	2	2	10	M	4	M	MxM
Insecure Neighbour Discovery	2	2	2	1	2	9	M	4	M	MxM
Buffer Reservation Attack	2	2	2	1	1	8	M	2	L	MxL
RPL Routing Attack	2	1	2	1	1	7	L	1	L	LxL
Sinkhole Attacks	3	1	3	1	1	9	M	1	L	MxL
Wormhole Attacks	3	1	3	1	1	9	M	1	L	MxL
Sybil Attacks on Intermediate Layers	3	2	2	2	2	11	M	4	M	MxM
Authentication and Secure Communication	2	2	2	2	2	10	M	4	M	MxM
Transport Level End-to-End Security	2	1	2	1	3	9	M	3	M	MxM
Session Hijacking	2	2	2	1	2	9	M	4	M	MxM
Session Establishment and Resumption	2	2	2	1	2	9	M	4	M	MxM
Privacy Violation on Cloud-Based IoT	2	1	1	3	3	10	M	3	M	MxM
CoAP Security with the Internet	3	3	2	3	3	14	H	9	H	HxH
Insecure Interfaces	2	3	2	3	2	12	H	6	H	HxH
Insecure Software/Firmware	3	3	2	3	2	13	H	6	H	HxH
Middleware Security	3	3	2	3	2	13	H	6	H	HxH

V. SECURITY

With the advancement of technology and its increasing use, issues of security and privacy become increasingly vital and major challenges. The elderly commonly lack understanding of complex technologies, the best practices to stay safe while using technologies, and the ability to deal with

[1] Future of an Ageing Population, Government report link

existential security breaches. Table II shows assets in home care automation [22], identified in terms of four key aspects:

- Behavioral competence: functionality in physical health, ADLs, cognition, and social behavior
- Environmental quality: relates to housing quality
- Perceived quality of life: perception of the surroundings individuals (family, friends, etc.)
- Psychological wellbeing: relates to mental health.

Different messaging protocols in IoT have various vulnerabilities, attributable to numerous reasons, including incorrect configuration or security services that pose security risks [22]. Some protocols, such as Constrained Application Protocol (CoAP), do not have any security protocols. Authentication and Security Layer (SASL) provides a greater number of setup options, which can lead to improper settings. Transport Layer Security (TLS) and Datagram Transport Layer Security are different from Internet Protocol (IP) traffic. Transmission Control Protocol (TCP) is used by TLS, while User Datagram Protocol (UDP) is used by DTLS. UDP is insecure in comparison to TCP [23]. Table III shows the main security of messaging protocols.

To identify risks concerning IoT, home automation technologies, patients, and home care providers, a risk analysis was conducted, to quantify risk in terms of the impact it causes on those assets. Table IV shows the risk evaluation and scoring. Risk can be modelled as shown below:

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

Where Likelihood = frequency × probability of a vulnerability's exploitation.

This means that the likelihood of a risk event happening is multiplied by the possible impact or harm the event could cause, which is used to determine the overall level of risk exposure. There are four essential steps of risk analysis:

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

The DREAD model uses a scaled grading system which assigns numerical data to risk categories to statistically evaluate the seriousness of a cyber threat. The DREAD model comprises five categories:

- Damage: Recognize the possible harm that a specific threat may cause.
- Reproducibility: Determine how simple it is to carry out an attack again.
- Exploitability: Examine the system's weaknesses, to see whether it is vulnerable to cyberattacks.
- Affected Users: Determine the number of users who might be impacted by a cyberattack.
- Discoverability: Evaluate how simple it is to find vulnerable points in the infrastructure of the system.

The DREAD model allows analysts to grade and compare the seriousness of threats by giving each of the aforementioned categories a score between 0 and 10. The ultimate grade, which is determined by averaging these category ratings, represents the risk's overall seriousness. The total threat rating is determined by adding the results for these five important categories. If the result was between 40 and 50 (Critical), the vulnerability is serious. If the result was between 25 and 39 (High), the vulnerability is severe, and should be considered for investigation and resolution soon. If the result was between 11 and 24 (Medium), the risk is moderate, and the review should be undertaken after dealing with severe and critical risks. If the result was between 1 and 10 (Low), there is a low risk to infrastructure and data.

VI. Conclusion

The analysis and assessment conducted in this paper can be used to determine how home care stakeholders understand and think about IoT technology. The results of this study can also be used to create a roadmap for those seeking to enter the IoT market. Through market research and industry analysis, this paper identifies potential benefits and risks for stakeholders, and discusses various applications of IoT technologies in elderly home care. This paper also discussed security in home care automation, and undertook a risk evaluation to offer an initial assessment for all involved stakeholders. Future work might consider different forms and design requirements, with a focus on usability and security, and move towards designing a framework to safely implement national IoT-based home care systems.

References

[1] M. N. Bhuiyan, M. M. Rahman, M. M. Billah and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10474-10498, July. 2021.

[2] X. Yang, D. Fan, A. Ren, N. Zhao, and M. Alam, "5G-Based User-Centric Sensing at C-Band," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 3040-3047, May. 2019.

[3] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. R. Choo, "Detecting crypto-ransomware in IoT networks based on energy consumption footprint." Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 4, pp. 1141-1152, 2017.

[4] 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.

[5] D. He, S. Zeadally, N. Kumar and J. -H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590-2601, Dec. 2017.

[6] T. Wang, Q. Wang, Z. Shen, Z. Jia, and Z. Shao, "Understanding Characteristics and System Implications of DAG-Based Blockchain in IoT Environments," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14478-14489, 15 Aug.15, 2022.

[7] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T. -H. Kim, "A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges," *IEEE Access*, vol. 9, pp. 25344-25359, 2021.

[8] A. Rajaiyan and S. Sobati-Moghadam, "Optimized Power Consumption Formula for Designing IoT-Based Systems," *2022 Second International Conference on Distributed Computing and High Performance Computing (DCHPC)*, 2022, pp. 74-77.

[9] Y. Ma, G. Ma and B. Ai, "Multicarrier Tandem Spreading Multiple Access (MC-TSMA) for High-Speed Railway (HSR) Scenario," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3490-3499, 1 March 1, 2021.

[10] H. Kim and J. Ben-Othman, "A Virtual Emotion Detection System With Maximum Cumulative Accuracy in Two-Way Enabled Multi Domain IoT Environment," *IEEE Communications Letters*, vol. 25, no. 6, pp. 2073-2076, June 2021.

[11] W. Zhang, J. Wang, G. Han, S. Huang, Y. Feng, and L. Shu, "A Data Set Accuracy Weighted Random Forest Algorithm for IoT Fault Detection Based on Edge Computing and Blockchain," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2354-2363, 15 Feb.15, 2021.

[12] M. Elkahlout, M. M. Abu-Saqer, A. F. Aldaour, A. Issa and M. Debeljak, "IoT-Based Healthcare and Monitoring Systems for the Elderly: A Literature Survey Study," *2020 International Conference on Assistive and Rehabilitation Technologies (iCareTech)*, 2020, pp. 92-96.

[13] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa and H. Song, "Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications," *IEEE Access*, vol. 4, pp. 6171-6180, 2016.

[14] KU, Sreekanth, and KP, Nitha "A study on health care in internet of things" *International Journal on Recent and Innovation Trends in Computing and Communication*, volume 4, pages 44–47, 2016.

[15] N. M. Allifah and I. A. Zualkernan, "Ranking Security of IoT-Based Smart Home Consumer Devices," *IEEE Access*, vol. 10, pp. 18352-18369, 2022.

[16] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating Smart Home Security: Is Blockchain the Answer?," *IEEE Access*, vol. 8, pp. 117802-117816, 2020.

[17] R, G. Marshal, K. Gobinath and V. V. Rao, "Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks," *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2021, pp. 1-4.

[18] S. M. Karunarathne, N. Saxena and M. K. Khan, "Security and Privacy in IoT Smart Healthcare," *IEEE Internet Computing*, vol. 25, no. 4, pp. 37-48, 1 July-Aug. 2021.

[19] "IBISWorld," *Domiciliary Care in the UK*, *Industry market research, reports, and Statistics*. [Online]. Available: https://www.ibisworld.com/. [Accessed 6 June 2020].

[20] "Network HSC," Home | Network HSC. [Online]. Available: https://www.networkhsc.co.uk/news/news-events/the-uk-home-care-market-explained/. [Accessed 6 June 2020].

[21] "NHS" Homecare providers in the UK. [Online]. Avilable: https://www.nhs.uk/conditions/social-care-and-support-guide/care-services-equipment-and-care-homes/national-homecare-providers/ [Accessed 5 June 2022]

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

[23] 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.