UK-RAS White Papers

ISSN-2398-4422
DOI: 10.31256/WP2023.1

UK-RAS NETWORK
ROBOTICS & AUTONOMOUS SYSTEMS

Security and Privacy in Assistive Robotics: **Cybersecurity challenges for healthcare**

www.ukras.org.uk

UK-RAS
NETWORK
ROBOTICS & AUTONOMOUS SYSTEMS

WWW.UKRAS.ORG.UK

FOREWORD

Welcome to the UK-RAS White paper Series on Robotics and Autonomous Systems (RAS). This is one of the core activities of UK-RAS Network, funded by the Engineering and Physical Sciences Research Council (EPSRC). By Bringing together academic centres of excellence, industry, government funded bodies and charities, the Network provides academic leadership and expands collaboration with industry while integrating and coordinating activities across the UK.

This white paper explores the security and privacy needs for Robotics and Autonomous Systems (RAS) working in healthcare. RAS devices in the care domain will enable people a greater degree of independence, with less reliance on other people, and this in turn could enable people to remain longer in their own homes.

People will be happier, healthier, have less financial burden on themselves as well as the UK as a whole. As a necessity for operation, care robots will collect data and information on the world around them to enable them to function safely, as well as a valuable source for medical diagnosis. But we need to be sure this information remains under controlled access as well as the type of information provided is strictly limited. I hope this excellent white paper will enable research and development to ensure the UK can benefit from the positive transformation offered from care robots, in a safe, secure and ethical manner.

The UK-RAS white papers serve as a basis for discussing the future technological roadmaps, engaging the wider community and stakeholders, as well as policy makers in assessing the potential social, economic and ethical/legal impact of RAS. It is our plan to provide updates for these white papers so your feedback is essential - whether it be pointing out inadvertent omissions of specific areas of development that need to be covered, or major future trends that deserve further debate and in depth analysis.

Please direct all your feedback to:
info@ukras.org.uk
We look forward to hearing from you!

Prof. Robert Richardson
Chair, UK-RAS Network

Prof. Alessandro Di Nuovo,
Professor of Machine Intelligence at Sheffield Hallam University.

Dr. Chris Elliott,
Founder & CEO of Pitchill Ltd.

Dr. Jims Marchang, Sr. Lecturer of Cybersecurity at Sheffield Hallam University.
(*Corresponding Author)

Dr. Helen Meese,
Founder & CEO of the Care Machine Ltd.

Dr. Samuele Vinanzi,
Lecturer in Robotics and Artificial Intelligence at Sheffield Hallam University.

Prof. Massimiliano Zecca,
Professor of Healthcare Technology at Loughborough University.

Other Contributors:

We would like to thank all the other contributors in shaping this white paper. We offer a special thanks to Prof. Angelo Cangelosi (University of Manchester), Prof. Steven Furnell (University of Nottingham), Prof. Christopher Dayson and Prof. Sally Fowler-Davis (Sheffield Hallam University), Dr. Daniele Magistro (Nottingham Trent University) for delivering expert talks on recent development in the robotic security, issues and challenges during the one day workshop on "Research Scoping of Security and Privacy in an Assistive Multimodal Robotic System (Health and Care)" and for sharing innovative research ideas. We also thank our industrial partner Ian Gardner FBCS CITP, Senior Account Technology Leader of IBM for enlightening us on "Securing your factory of the future". We thank Dr. Guodong Zhao (Glasgow University), Mr. Erioluwa Adeola (Loughborough University), Prof. Francisco Javier Aparicio Navarro (De Montfort University) and Mr. Raymond Mawanda for presenting their research findings and sharing ideas during the workshop. We also appreciate the contribution of Dr. Liang Chen (University of Hertfordshire) and Dr. Ben Sanders (Winchester University) for support during the development and drafting of the white paper.

Finally, we would like to give special thanks to the Darnall Wellbeing Staff and the community of Sheffield, Public Involvement in Research Group (PIRG) of Advanced Wellbeing Research Centre (AWRC) of Sheffield Hallam University (SHU), and other communities of Sheffield and South Yorkshire. This is for actively participating in the public engagement events and in the research by filling in a questionnaire for analysing security and privacy needs for public acceptance of care robots.

EXECUTIVE SUMMARY

This white paper investigates and highlights the security and privacy needs, issues, and challenges for Robotic and Autonomous Systems (RAS) applied to healthcare environments, and how these issues can impact the end users' trust and adoption of this technology. To this end, we conducted a critical literature study in this domain, with questionnaires and feedback analysed from potential users (patients and social care workers), stakeholders (doctors, care providers, etc.) and experts from both academia and industry in the field of Cybersecurity, Artificial Intelligence (AI), and Robotics.

The results of the analysis indicate that to design, develop and implement intrinsically secure RAS, the system designer and developer should adopt the following key strategies:

- The RAS should be secure by design so that security features are added from the start and not added after the development of the system.
- The RAS should be privacy by design to safeguard the privacy of the user from the start of the design and the development of the RAS to guarantee the privacy of the user.
- The care RAS system should be transparent so that it is auditable and traceable.
- A careful trade-off between the quality of the RAS service delivery and system overheads should be considered in designing and developing care RAS to ensure a real-time response.
- To make RAS adoption acceptable and usable with ease, personalised user-centric security and privacy mechanisms and techniques should be developed, while the underlying security complexity should be concealed to avoid them being perceived as barriers and burdens.
- New Government laws, policies, regulations, and compliances need to be developed to oversee the safe adoption of this new era of AI-based care RAS solution in healthcare to strictly comply with the UK General Data Protection Regulation (UK GDPR).

We conducted a public engagement survey for wide-reaching of potential users with Darnall Wellbeing Staff and the community of Sheffield, Public Involvement in Research Group (PIRG) of Advanced Wellbeing Research Centre (AWRC) of Sheffield Hallam University (SHU), and other communities of Sheffield and South Yorkshire. The survey results showed that 100% of respondents agree that secure RAS and user privacy are essential for the safe adoption of this technology. These results highlight the importance of considering security and privacy in the design and development of RAS to promote widespread adoption.

Overall, this white paper highlights the critical need for secure and private RAS in healthcare environments. By adopting the key strategies outlined above, we can improve user trust and acceptance of RAS while promoting compliance with data protection regulations. Conversely, underestimating these aspects during the design and development of RAS might have serious repercussions for their widespread adoption.

> To enhance trust in RAS adoption, the users must know how the system agent takes decisions.

CONTENTS

1. INTRODUCTION

Governments across the world are struggling with the growing crisis in demand for supporting people as they get older. The United Nations Population Division reported in 2019 that there will be a 120% global increase in the number of adults aged over 65 years by 2050 [1]. Practical solutions to this crisis must be found.

Among ageing populations, where older people prefer independent living but where there is a shortage of care providers, assistive robotic systems (or care robots), are a potential solution to maintain good quality living among older people, and differently-abled people (such as a different learning ability or physical ability due to a medical condition) and support them towards independence in overcoming any barriers in their daily activities. Indeed, the robotic nursing assistance market has been valued at $975.6 million in 2022, and the revenue forecast by 2030 is $2.93 billion [2]. It is crucial therefore not only to invest in this kind of technology but also ensure that it is accessible and acceptable by securing and protecting users' data and privacy.

The UK Houses of Parliament [3] reports that integrating more robotics in the UK health and care system may save up to £6 billion through automating some tasks. However, concerns about user privacy and questions over the use and ownership of data still remain.

1.1. WHAT IS A CARE ROBOT?

The healthcare sector presents particularly unique challenges for research on Robotic Autonomous System (RAS) compared to other domains. This is because the smart systems and devices being developed manage sensitive and private data about patients that must be protected from being inadvertently disclosed. This vulnerability will have a significant impact on users' acceptance and adoption, especially considering the already low level of trust in AI and autonomous systems.

A care robot is an intelligent machine designed to assist and support older or disabled people, improving their wellbeing and quality of life. Robots providing physical assistance have been shown to increase users' autonomy and dignity by assisting with tasks like feeding, washing, and walking, and are being developed to support physiotherapy [4].

Socially assistive robots (SAR) provide novel opportunities for aiding daily living activities, such as reminding users to take their medicine, and detecting and preventing falls. SAR is a more ambitious system, which includes support for complex functionalities such as dexterous manipulation, advanced navigation, and a natural, more intuitive interface, which can overcome some of the difficulties currently experienced, especially by older people [5]. On the other hand, Robot-led psychometric assessment could have many advantages, such as wider availability, test standardisation, and assessor neutrality while providing higher engagement and usability to people with limited digital literacy [6]. Social robots can provide a solution for the challenges of an ageing population, in particular, to reduce social isolation and loneliness [7]. Researchers are also exploring the use of multi-robot systems, integrated into smart homes and intelligent environments, which are able to coordinate with each other to better perform their tasks, also outside the home. These advanced systems could provide continuous support in a variety of daily activities, thus, enabling older people to live independently at home for longer. A pilot conducted by Hampshire County Council found that the use of Amazon Echo did result in a reduction in users' self-reported feelings of isolation and loneliness [8]. Also, robotic pets introduced in one UK care home were reported to bring happiness and comfort to residents [9]. A few examples of RAS are shown in Figure 1, Figure 4, Figure 6, and Figure 9.

Figure 1:
Care-O-Bot Arms and Legs of Advanced Wellbeing Research Centre (AWRC), SHU, Sheffield, 2022.

1.2. IMPORTANCE OF SECURITY IN HEALTHCARE ROBOTS

As reported in the IBM Security X-force threat intelligence index [10,11], the healthcare sector is the 6th and 7th most cyber attacked industry in 2021 and 2022 which amounts to 5.10% and 5.80% respectively of all known cyber-attacks. In addition, among all forms of cyber-attacks, vulnerability exploitations are the most common cyber-attacks in the healthcare sector, constituting 57% of the total, followed by 29% in phishing and 14% in credentials theft. However, globally, Europe has the lowest healthcare percentage of attacks amounting to only 6%, while most attacks happen in the Middle East and Africa, accounting for 39%. North America amounts to 33% while Asia and Latin America stand at 11% each. In another research report produced by IBM Security, Cybersecurity Intelligence group, it is found that over 95% of cyber security incidents are due to "human error" [12]. The most common errors include system misconfiguration, poor patch updates, use of default or easy access credentials, disclosure of information, and so on. The chances of such errors will only increase when these systems are utilised by older people who have medical and physical or psychological conditions.

It is important to note that "Older people become victims of fraud every 40 seconds" as reported in Age UK's research findings [13]. So, securing and preserving users' privacy using innovative, smart, intelligent (easy to adopt and easy-to-understand) solutions is vital to ensure that the user's fault and error do not impact the RAS or its data. Thus, RAS should be secure by design and privacy by design. This means that security and privacy should not be treated as separate applications but instead be built into the system from the outset. Further, the systems in place should be resilient from cyber-attacks and reduce the potential for human error whilst increasing the benefit for the user, RAS and the data it stores.

Moreover, specific solutions for system security, safeguarding users' privacy, and data security aspects for RAS applications in healthcare have not been fully explored yet, especially in terms of communication protocols. Indeed, securing such multimodal systems is challenging because there are many data leakage points. Communication and connection from connected sensors and cloud services to the robotic system need to be protected to maintain data integrity, data confidentiality, and data availability. One of the reasons why security and privacy preservation has not received sufficient attention in RAS is mainly due to two factors: Firstly, research seems to be mainly focused on enhancing the functionality of robotic hardware and software; secondly, tackling security issues in this context requires a highly interdisciplinary set of skills and collaboration between diverse groups of experts (namely, Cybersecurity, Networks, AI, Robotics, and Healthcare). However, the need for a wide range of skills in developing security and privacy solutions should not be a hindrance to users. Instead, the solution should be user-friendly, easy to adopt, and trustworthy.

> "The healthcare sector is the 6th and 7th most cyber attacked industry in 2021 and 2022 which amounts to 5.10% and 5.80% respectively of all known cyber-attacks"

as reported in the IBM Security X-force threat intelligence index.

> Older people become victims of fraud every 40 seconds
>
> as reported in Age UK's research findings.

1.3. TRANSFORMATION OF ASSISTANCE THROUGH CARE ROBOTS

Digital technology and innovation have transformed healthcare systems across multiple dimensions and have been successfully tackling challenges on shortages of carers and improving the care service quality. The care services' limitations and support challenges were brought to the fore during the COVID pandemic. Digital solutions are increasingly being adopted and are transforming the way services are provided as outlined in several papers [14-17]. Smart and intelligent digital systems can enable and support older and less-abled individuals and provide quality living by empowering people to have choice and control of their lives with the reduced need for assistance from another person. As reported by the United Nations, Department of Economic and Social Affairs, Population Division [18], older people in Europe and Northern America prefer to live independently unlike other parts of the world, so smart technology innovations like smart home appliances, driverless cars, and assistive robotic systems can support quality independent living. A growing body of research shows that assistive and social robotic systems can address and have the potential to augment healthcare providers to support the physical, cognitive, and social needs of older people [19-23]. However, acceptance and positive responses from older people about robotic design, methods of communication, and interaction are key for successful implementation and adoption [24]. Even though assistive robotic systems can improve the quality of independent living and can be a step-in to support carer shortages across the ageing countries, this technology has several issues and concerns regarding its acceptance concerning ethics [25-27]. In addition, it has a serious user data privacy issue when dealing with intelligent assistive social robots that incorporate conversational agents [28]. Because of this, a secure-design robotic system should be a mandatory requirement to support and provide independent quality living for the older generation as shown in Figure 2.

Security and privacy mechanisms in assistive RAS should not hinder the user's experience, irrespective of their health, physical or mental conditions including and not limited to people who are autistic, have learning or physical disability, mental health conditions, sensory impairments, dementia, or any long-term conditions. The user and its assistive RAS engage with different types of people, directly or indirectly, including care workers, personal assistants, social workers, therapists, nurses, doctors, family members, and even system engineers for maintenance. The level of access needed and the information available to them depends on their role: it is vital to make only the essential data visible to them to preserve the user's privacy.

Figure 2:
Aiming to Support Independent Quality Living of the Older People (First Photo[1], Second Photo[2] and Third Photo[3])
[1] https://unsplash.com/photos/P5c4cgJgg3g [2] https://unsplash.com/photos/GgRlUhPrCPw [3] https://unsplash.com/photos/TeWwYARfcM4

2. SECURITY, PRIVACY, AND TRUST FACTORS FOR CARE ROBOTS

When securing care RAS, it is critical to understand the users that are involved in dealing and engaging with the RAS and it is also important to consider all the factors that affect user's trust. During the development of care Robots, it is critical to understand the key parties involved such as the user and the third parties apart from the Robot itself to understand the security needs, its importance, its complexity, and how the Robots need to be made transparent to maintain the user's trust.

2.1. PARTIES TO SECURE (RAS, USER'S DATA, THIRD PARTY)

During an interaction between users and a RAS, multiple parties need to be protected to ensure data confidentiality, integrity, and availability: in particular, the robotic system itself, the smart IoT devices and cloud services that might support the intelligent agents, and, finally, the users themselves, including their data. The RAS users' needs, and requirements are different even if they are all authorised to access the same system. Types of users include the owner (the main user or users), management team, and user support team (family members, cleaners, carers, and health professionals such as nurses or doctors). Depending on the need and requirement of each user type, different access levels should be granted. The security and privacy protection mechanisms are a core requirement for any interaction and engagement between the RAS, Users, and the Third-Party Service (Smart IoT integration and Cloud services) as shown in Figure 3 and this idea is captured in the previous work of the authors' [37].

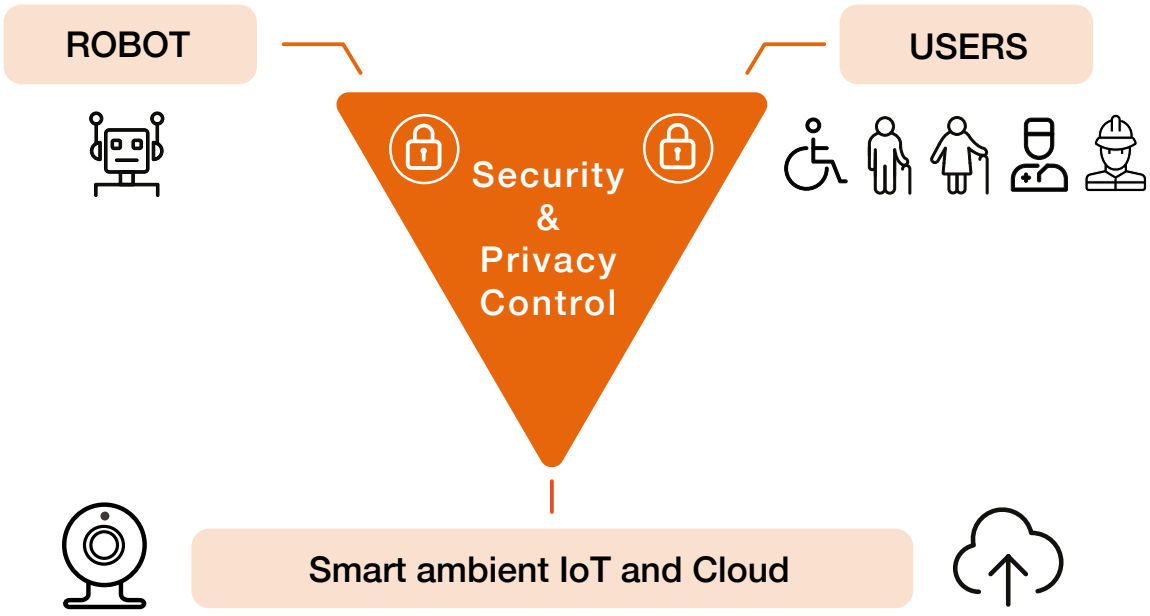


Figure 3:
The RAS Triangle Security Association

2.2. BUILDING TRANSPARENT CARE ROBOTS TO GAIN TRUST

When RAS provides service and care to users, it is important for it to be transparent. This allows it to be accountable, follow precise regulations, and be certifiable, explainable, auditable, and scrutable [29]. Blockchain technology (BCT) might be considered a new potential tool for RAS because of its capacity to ensure data and storage transparency, making it tamper-proof and traceable [30,31]. However, BCT is resource hungry, so it would be a daunting task to integrate it within a RAS, which is already computationally intensive on its own. Smart home (smart IoT sensors) and well-being sensors integration with RAS will enable the latter to make well-informed decisions and reduce its computational overheads while interacting with the smart house, smart wearables, and the user. Moreover, when a computationally intensive RAS is integrated with both a smart IoT network to reduce its computational overhead and with BCT to ensure transparency, it is crucial to maintain a trusted relationship between the smart home network and the RAS (e.g., sensory device and its data confidentiality, integrity, and authenticity must be always maintained) and preserve users' data privacy in the process. To enhance trust in RAS adoption, the users must know how the system agent takes decisions. This is done because maintaining transparency is a way to make every action of RAS accountable and in turn, it will make the system explainable, auditable, and scrutable. However, in the process of making the system transparent, the overhead of computation and memory or storage requirements should not negatively impact the user experience and privacy.

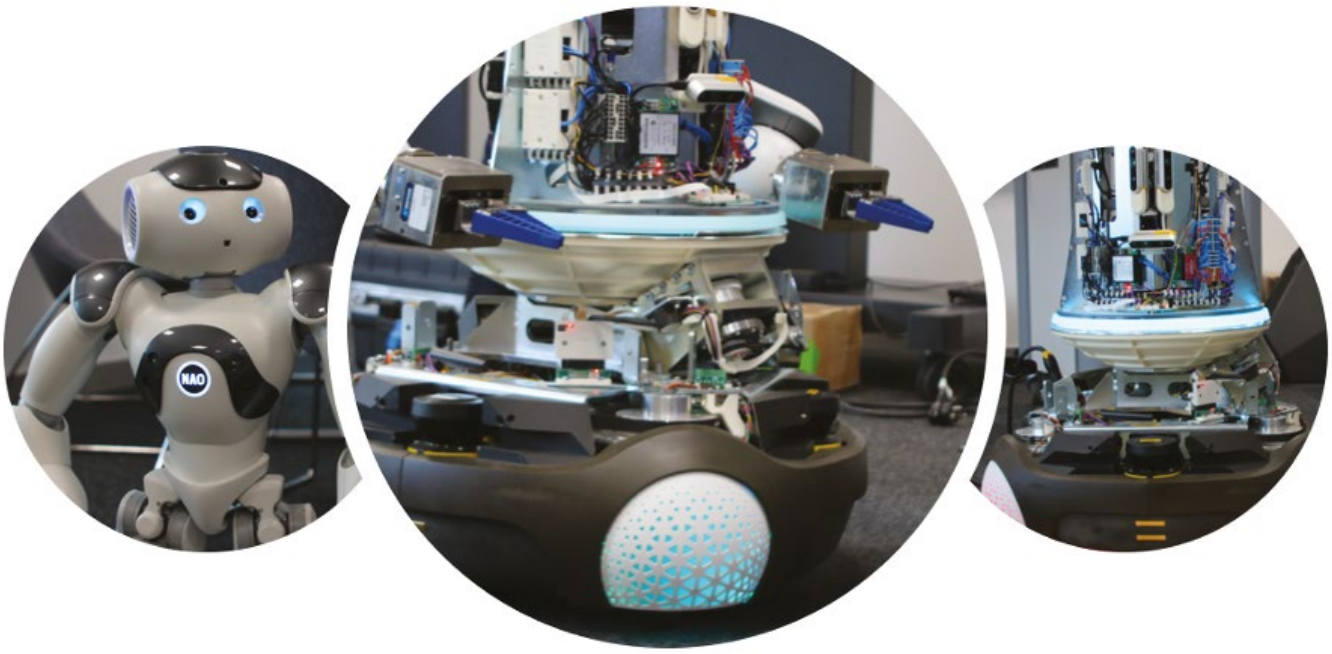


Figure 4:
NAO and Care-O-Bot Internals of Advanced Wellbeing Research Centre (AWRC), SHU, Sheffield, 2022

2.3. WHY IS RAS NOT SAFE WITHOUT SECURITY AND PRIVACY PROTECTION?

In designing and developing RAS, without security and privacy mechanisms in place, multiple issues will arise and threaten RAS functionality and its adoption:

- RAS and user's data confidentiality will be compromised (anyone can see)
- RAS services, data integrity, and data reliability are not preserved (data tampering or modification will happen)
- RAS services and data availability are not guaranteed (unable to access information)
- Unauthorised users can access RAS and its services, and all personal and private data will get leaked (anyone can access user data and RAS service anytime)
- Third parties (cloud service providers, workers, and carers) could steal users' information and misuse it (cannot trust anyone)
- No boundaries and limits on accessing data and services among different kinds of users, such as workers, doctors, engineers, and family members (anyone can access any data)
- RAS can be weaponized (its data and services can be manipulated, and actions can be controlled)
- RAS will be open to hackers and any form of intrusion (bots to malware to a virus)
- Users' data and RAS will be an open system to anyone and everyone (no privacy or no consent or no user rights on their data and their personal RAS).

2.4. THE COMPLEXITY AND IMPORTANCE OF SECURING AND PRIVACY PRESERVATION IN CARE ROBOTS

Privacy is a way to protect individual rights. If somebody extracts, sees or intrudes on someone's life or personal information without having access rights and consent, this will be considered a breach of their privacy. In a multimodal RAS, there are different ways through which the robotic system's security and privacy could be compromised, and there are multiple factors that might create a bottleneck in integrating security features. Moreover, privacy is complex, and defining it is a daunting task because it takes on different meanings and is highly subjective. A historical Harvard Law review [32] defines privacy as the protection of an individual's personal space and their right not to be intruded upon and to be left alone. Schoeman [33] argues that privacy is an aspect of one's dignity, autonomy, and freedom. Privacy issues and challenges are a multidisciplinary subject that overlaps with various fields of study including economics, management, law, sociology, and psychology [34]. In this technology-driven data world, studies define privacy as means to control, safeguard, and protect one's information [35]. When it comes to information privacy, it allows individuals to control when, where, how, and to what degree personal information is released or shared with others [35]. Privacy is critical because it is linked with ethical, legal, social, and political issues in this era of information technology. The revised GDPR, 2018 [36] aims to inform EU citizens and businesses on how to collect, use, share, secure, and process personal data. However, the fast-changing technology makes it very challenging to comply with the regulations since the way information is collected, stored, processed, and transmitted changes constantly and is also affected by the specific technology which is involved (for example, RAS versus web-based instruments).

In an assistive multimodal RAS, securing and preserving users' privacy is complex due to the nature of its multimodality. However, it needs to be addressed to maintain users' trust.

> "Privacy is critical because it is linked with ethical, legal, social, and political issues in this era of information technology."

2.4.1. Critical Security issues to be considered

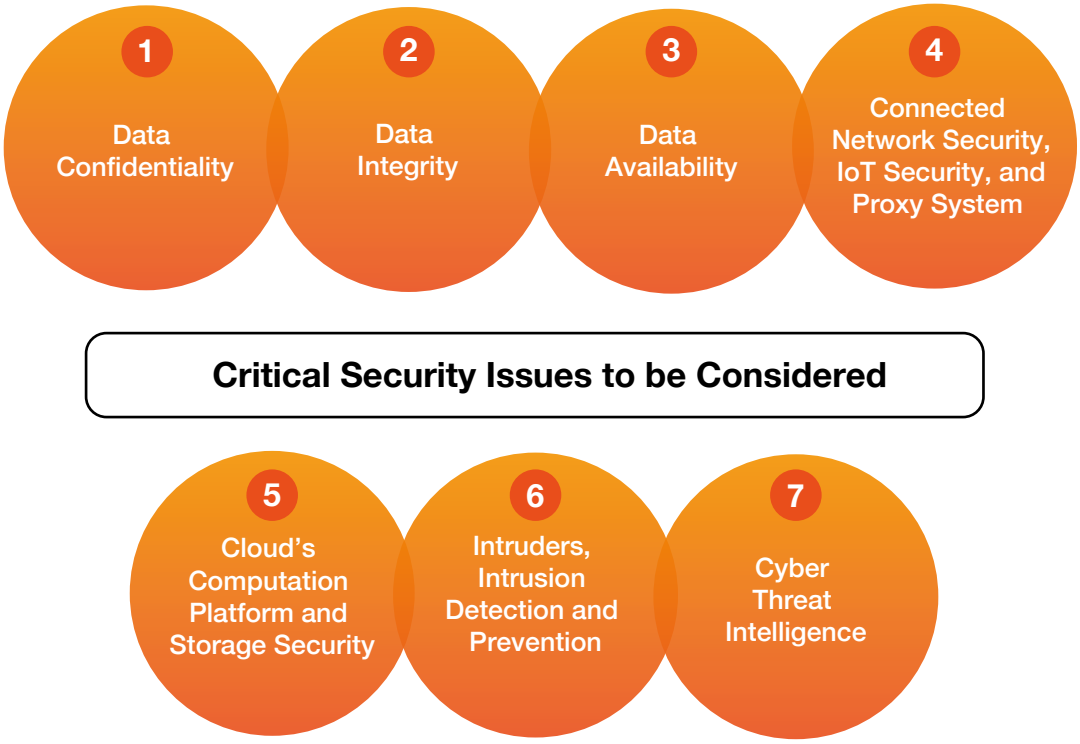


Figure 5:
Critical Security Issues to be Considered.

The importance of security and privacy of the user, its data, and care RAS has highlighted some of its key issues, and challenges, and provided some possible security solutions and directions for assistive multimodal robotic systems [37]. Other research [38] reinforces the importance of security and privacy by proposing and providing directions on how to conduct access control through task planning and activity-centric execution in assistive robotics, strengthening the idea that these must be enforced and guaranteed by any RAS. Multiple factors could make a robotic system vulnerable: impersonation, man-in-middle attacks, and software and operating system bugs are just a few examples. The highlighted issues and challenges are vital for protecting and safeguarding RAS and its users. There are multiple dimensions and aspects that need to be considered when securing the RAS system and they are highlighted in Figure 5. The following security features and domains are key to keep RAS safe and secure:

1. Data Confidentiality: Interaction and engagement between the user and the RAS could be conducted in multiple ways (voice, sign, and signals, apart from using devices, web, app, etc.). Maintaining data confidentiality using traditional cryptographic methods will not apply especially when the communication involves visible gestures and audible voice, but the system must find different ways to maintain data confidentiality.

2. Data Integrity: It is mandatory to ensure the reliability of the data against any form of data tampering and prevent any form of data alteration during data transmission or data storage.

3. Data Availability: The stored data should be accessible for all authorised users and partners and the security mechanisms should not affect any authorised user's attempt to access their data.

4. Connected Network Security, IoT Security, and Proxy System: When RAS is connected to a cloud system for processing or storage, and when it communicates with remote stakeholders for monitoring or control, traditional security mechanisms will work, but providing and ensuring security will be challenging especially when it is coupled with low powered resource-constrained smart IoT systems (smart home and well-being monitoring system) for RAS' optimisation and performance reasons.

5. Cloud's Computation Platform and Storage Security: To preserve user confidence, cloud, and storage security are important whether RAS data computes and stores locally or over the cloud. Cloud computation and storage services should not allow any unauthorised access to users' data. Novel security frameworks that are easily controllable, adoptable, and manageable based on the user requirement need to be developed.

6. Intruders, Intrusion Detection and Prevention: Any device, system, or person (adult or minor) aiming or planning to listen, observe, steal data, tamper with, or destroy information is an intruder. Defining boundaries and understanding who is authorised, who can access what information, and what service, and defining access limits and rights are critical in detecting and identifying intruders. A multimodal assistive RAS should not only aim to detect and expel intruders but also detect them in real-time to minimise any cyber breach impact.

7. Cyber Threat Intelligence: The RAS should collect, observe, and analyse data to be able to understand the motives of an attack, and the behaviour of the attackers and to provide necessary intel that will guide the future refinements of the security measures, in an ongoing development process.

Figure 6:
Pet Robot and NAO Robot of Advanced Wellbeing Research Centre (AWRC), SHU, Sheffield, 2022

2.4.2. Privacy Concerns

Privacy concerns of the users are real, and RAS should apply all the necessary techniques to protect user privacy and the areas of privacy concerns are listed in Figure 7. There are diverse ways through which the privacy of the users could be compromised: (1) Unintended Data Disclosure Issue: Unless the RAS is made aware of what service to provide when and where it might easily leak private information of the user in public places or in the presence of other users; (2) Inappropriate Data Disclosure Issue: Due to unawareness of the RAS, it could easily discuss, share, or engage with the user in presence of an unintended or inappropriate audience (e.g., in presence of a child). Training the RAS to consider what is appropriate to share and acceptable to whom, where, and when is a complex issue that needs to be addressed; (3) Access Control (Identification, Authentication, Authorisation, including Accounting): To guarantee that only the authorised users can access RAS and its services and to protect user privacy, user data, and the RAS itself, it is vital to control the access of the RAS services, its stored data, and its service privileges based strictly on need and requirement basis; (4) Seamless Continuous Authentication for Access Continuity: A development of Continuous authentication techniques which will not be a barrier or burden (irrespective of the user's physical, psychological, or physiological state?) to the user is mandatory, otherwise, RAS could be left open with an opportunity for unauthorised users to access the system if a traditional one-time authentication technique is adopted (be it single or multifactor); (5) Disciplining RAS: During the engagement and interaction with the user in the presence of friends, families, or the public, the RAS must be disciplined, otherwise, user privacy might be compromised. In addition, the privacy mechanism should not offend, embarrass, or annoy either the user or other people around the user; (6) User Constraint: Security solutions should consider user's psychological, cognitive capacity, technical abilities, or physical conditions to safeguard user's privacy; and (7) Scalability and System Constraints: Security mechanisms incorporated in making the RAS secure and private should not affect user's interaction and engagement experience. Moreover, in a social care environment, RAS should be able to support multiple users, and be able to protect and preserve each user's privacy while ensuring a high-quality user experience.

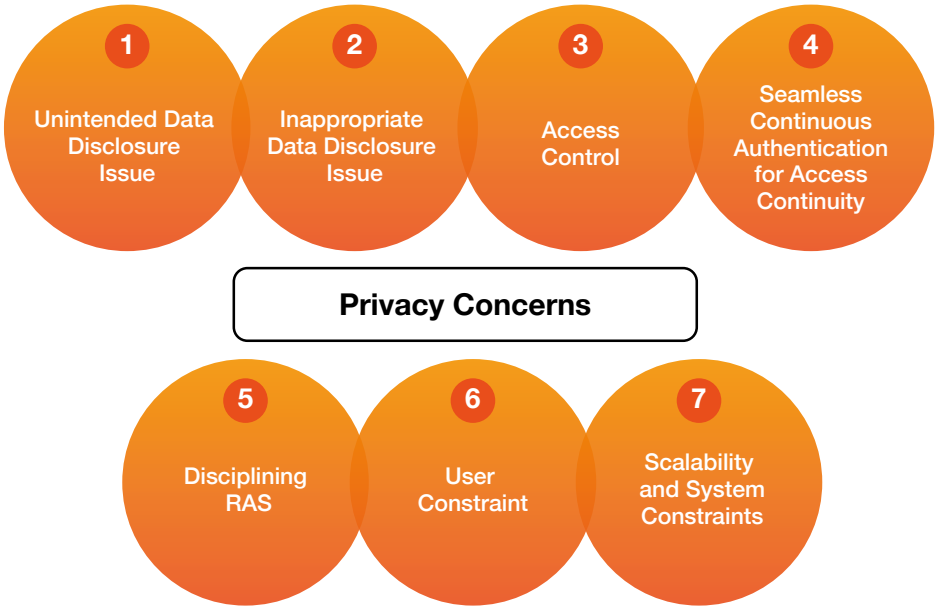


Figure 7:
Areas where User's Privacy could be Compromised

3. USER AND DESIGN PERSPECTIVE

During the design and development of RAS, it is critical to consider users' preferences, RAS capability and security overheads. This is to ensure that the RAS is usable to anyone with any physical or mental abilities, it is cost effective and secure at the same time. Moreover, the security and privacy mechanisms should be incorporated during the design and development process.

3.1. USER-CENTRIC CO-DESIGNING SECURITY SOLUTIONS

The security issues of RAS cannot and should not be conceived or perceived only as a technical cybersecurity problem. To address the problem holistically, it is critical to understand both the psychological and physiological needs and conditions of the RAS users and the trade-off between security mechanisms requirements and computational resource constraints (computation, memory, storage, and network bandwidth requirements). The security solution may not be adoptable and acceptable to the users due to their mental or physical needs and their abilities, and it may also become a bottleneck towards real-time response, other than affecting the user experience. Therefore, socially acceptable, and adoptable security mechanisms and techniques should be inclusive of cognitive impairment, mental issues, and physical disabilities of the users.

In the process of designing security solutions, it is important to adopt a user-centric design approach. In sum, designers should take into consideration the needs and capabilities of the user, the RAS resources capability, and, finally, the acceptable security overheads that strike the correct balance between safety and optimal user experience. This relationship between RAS resources, User needs, and ability and security overhead is shown in Figure 8 and based on the previous work of the authors [37]. Thus, security mechanisms should not interfere with the user experience on one hand, and on the other hand, they should not overwhelm the RAS with additional overheads.

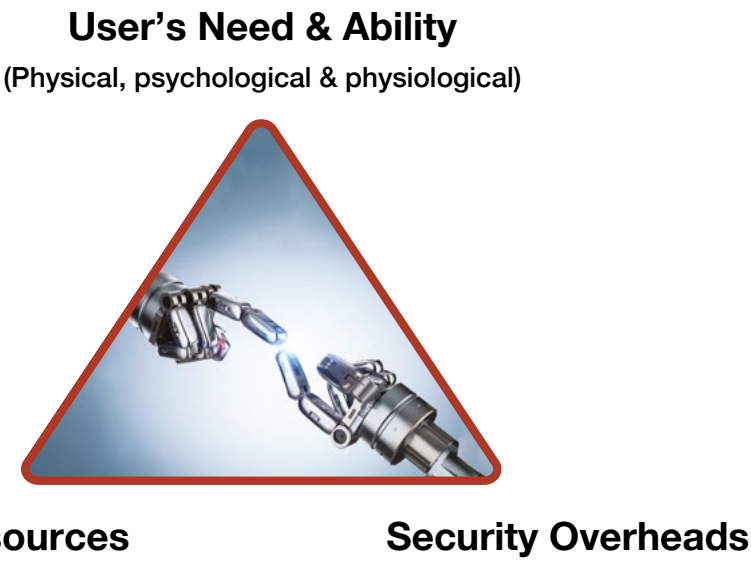


Figure 8:
User, RAS, and Security Association

3.2. SECURE AND PRIVACY BY DESIGN SECURITY SOLUTION

The Robot Operating System (ROS), one of the most adopted middleware for robot programming, runs within Unix-based operating systems, such as Ubuntu and Debian. ROS has no inherent security mechanisms: if the developers want to add them, they will run as applications inside the environment. An early study [39] aimed to highlight the importance of integrating security features in the kernel from the application level. Securing the communication and maintaining data integrity between nodes and modules functionalities needs to be integrated along with the security mechanisms in the design of ROS which is critical for secure by design solutions. There is also a need to secure ROS, including its sensory nodes, its application functions, storage, and any form of an external connection. In addition, the sensory devices connected to a robot should also be secured and authenticated for the user.

Challenging questions are raised when incorporating security and privacy mechanisms and policies in the RAS design and development:

- Who can access what resources and services from the RAS and what kind of boundaries need to be integrated into the secure design policy?
- Regarding updates, what components can be affected, when, and how?
- How to manage, exchange, and update certificates and keys?
- How should RAS engage with authorised and unauthorised users?
- How and when RAS data and services are shared and with whom and at what level?

All these aspects need to be included during the design and development so that such security and privacy features are not added over the application separately, but rather integrated within the system itself. An internal sensory network system of a Care-O-Bot is shown in Figure 9.

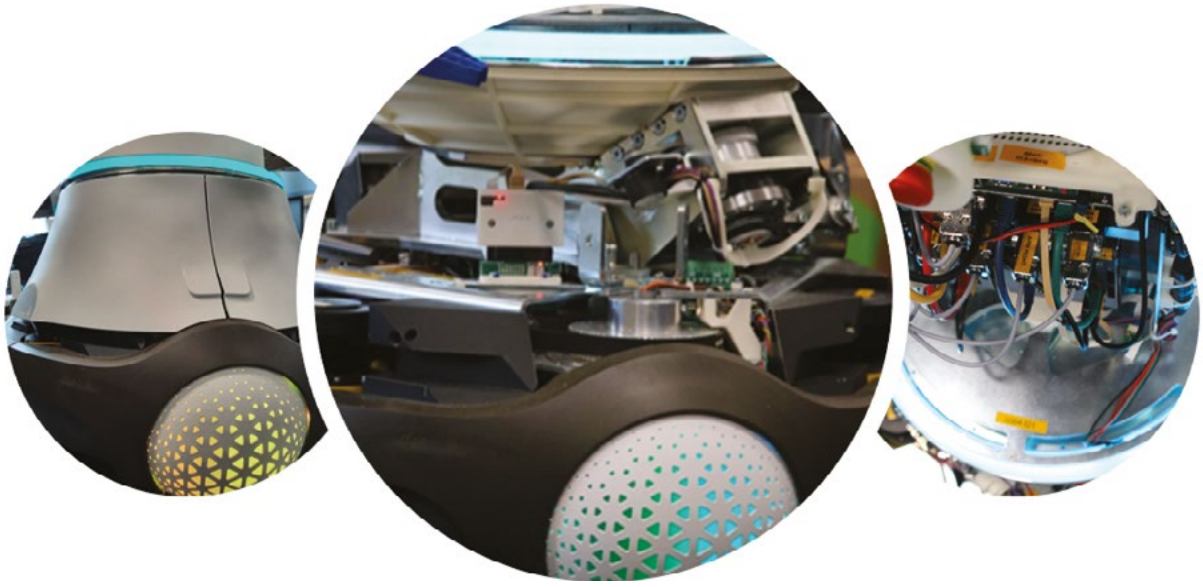


Figure 9

Care-O-Bot Internal Sensors and Connections, Advanced Wellbeing Research Centre (AWRC), SHU, Sheffield, 2022

4. CYBER IMPACT AND REGULATIONS NEED

Cyber threats are real and are disastrous. They could potentially lead to malfunctioning of the system, loss of information and communication, tampering user's data, misguiding the system and so on. So, it is critical to understand and explore all the key details of the impact of cyber threats on RAS. To guarantee that the manufacturers and the developers consider ways to secure RAS, user's data and user interaction and engagement with the RAS, it is mandatory to create new policies, regulations, laws, and compliances to ensure its safe development and deployment.

4.1. CYBER THREATS AND THEIR IMPACT

In the RAS ecosystem, cyber risks can happen at different levels and the level of cyber threats can damage and impact user's trust and confidence in RAS adoption. This can affect not only the RAS, its users, and the data, but also the entire network system, making it unreliable and not trustable. The system must be able to detect and withstand ransomware attacks, server compromise, data theft, credential harvesting, misconfiguration, malicious insider activities, etc. The following entities will be impacted when the cyber threats are not managed, or risks are not mitigated. Some of the key attacks and possible impacts are highlighted in Table 1 and based on the authors' work [37]. Cyber threats will have a huge impact on the RAS system's network operation, functionality, and control on one side, and on the other hand user's data secrecy, integrity, and availability cannot be trusted and reliable.

Attack On RAS	Impact
Confidentiality: - Key hijack, - key compromise - certificate attack, - Reconnaissance	Data would be visible and available to any third party and there would be no privacy on the user's data.
Integrity: - Non-repudiation, - Digital signature attack	Data could be manipulated, altered, tampered with, and modified.
Availability: - DoS, - DDoS, - Jamming, - spamming, - Black hole, - Wormhole, - Sink hole etc.	The RAS system could be shut down and made inactive and un-operational.
Access Control: - Dictionary attacks, - Brute-force attack, - Man-in-middle, - Phishing, - Keylogger attack, - Password Spraying attack	User identity would be compromised, unauthorised users would access the RAS services and data would become visible unless stored securely.
Storage/Memory: - Storage account discovery, - Data Deletion, - Data Alteration or Modification	Data visibility, manipulation, deletion or addition, corruption, and alteration.
Services: - Malware, - viruses to induce malfunction	The RAS and its services may stop working as intended.
Sensory: - Replacement, - Replication - Tampering, Identification	The sensors belonging to both the RAS and the smart environment can be manipulated. Data collected from unauthenticated sensory devices are unreliable.
Network: - Attack on Proxy server, - Man-in-middle attack, - Routing attack, - Media Access, - ARP attack, - Buffer overflow attack	When the RAS is connected to Cloud servers and smart IoT home systems, transit network data could be intercepted and captured, routing could be manipulated and exhaust network resources by denying services, and even the network connection could be disrupted.

Table 1: Cyber Attack Assessment on a RAS

4.2. NEW GOVERNANCE POLICIES, REGULATIONS, LAWS, AND COMPLIANCES

Proper governance of care RAS will contribute to two goals:

- Ensuring that the users and others trust the integrity of the data in the system. Although this is essential if people are to benefit from the capability, in practice, people are willing to tolerate poor privacy in exchange for a convenient service – e.g., the acceptance of Alexa or the willingness to check "I agree" on a software license without reading it. But that could be disastrous in the RAS eco-system because it deals with sensitive personal and private data.
- Ensuring that the system complies with the legal requirements. Privacy laws are strict and complex, and the penalties for breaching them can be significant. For the avoidance of doubt, the data generated by a care RAS will be subject to privacy laws in the UK.

The governance system needs to define how the system is designed and if data privacy is preserved, who should have access to which data, and how that access is authorised and controlled. Moreover, only the private data related to the RAS service is shared or engaged with any RAS stakeholders and new rules should be developed to cover the GDPR aspects on laws, regulations, compliances, governance, and policies.

Anonymisation is a robust form of data protection but is not appropriate when the purpose is to associate data with an individual. Pseudonymisation is a powerful halfway solution, where the data is anonymised but the anonymisation may be reversed by a key. Although it is hard to define the limits of pseudonymisation in a formal statute, there are helpful guidance documents (e.g., Information Commissioner's Office [40] or the EU Agency for Cybersecurity [41]).

From a legal perspective, the issue is complex. The UK's legal regime rests on the Data Protection Act 2018 and the UK General Data Protection Regulations, which currently mirror the EU's GDPR Regulation 2016/679. The Information Commissioner's Office has produced useful guidance [42]. However, the UK's regime may change as the effects of Brexit ripple through - it must balance its desire to create its own regime with the need to exchange data with the EU. However, the legal regime is universal, and it should apply to most if not any organisation that handles personal data. When RAS is deployed in a caring environment dealing with multiple users, RAS needs to ensure and guarantee the privacy of all the users it engages and interacts with.

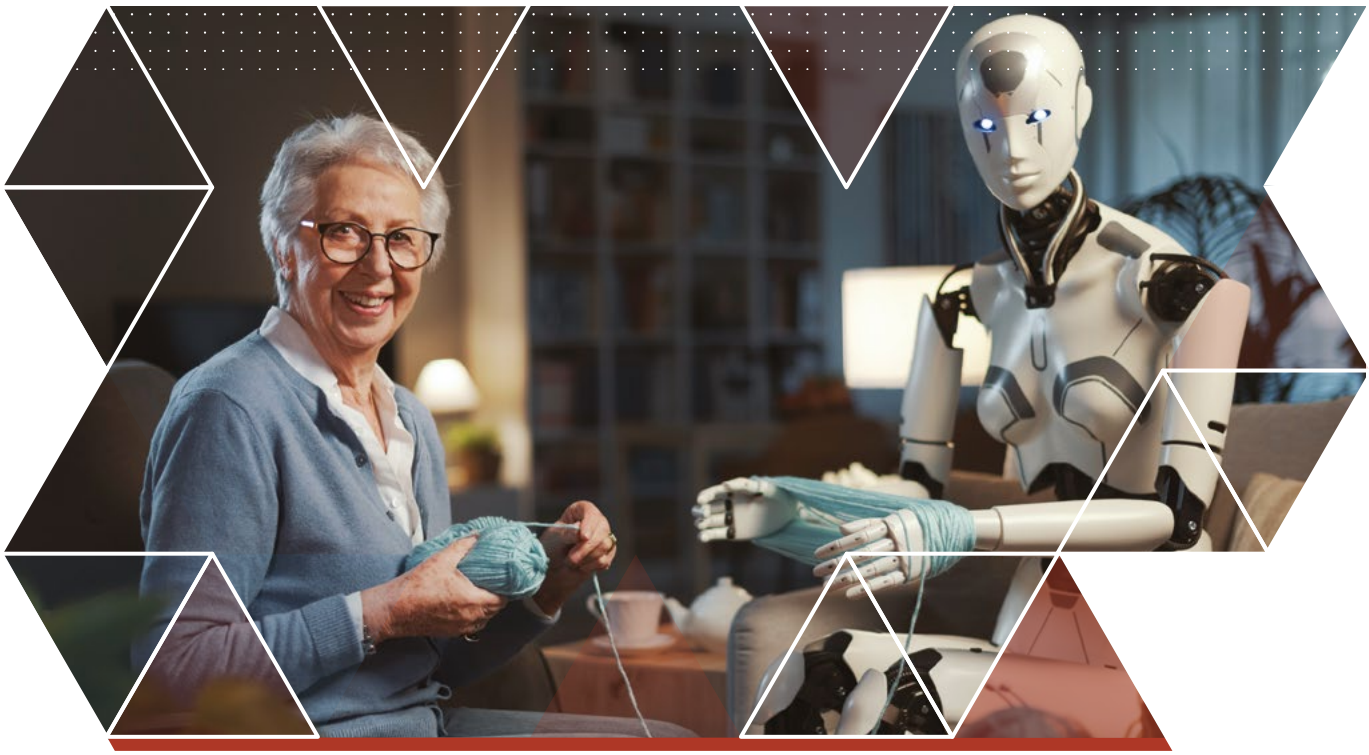
How the data is collected, how it is processed, how it is stored and how it is shared, and with whom are critical, and they must comply with the regulations of the region. E.g., Personal data held on a server located in the USA might be in breach of the law, and a server located in the EU might bring the EU's GDPR into play even if the data that it holds is owned by a UK company and that data only concerns UK citizens.

Thus, GDPR recognises two roles in the handling of data:

- Controller - the person that decides how and why to collect and use the data. The legal liability lies with the controller, which for a care RAS would most likely be the organisation that administers the care and operates the robot – not the manufacturer or supplier of the robot.
- Processor - a person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. This might include a cloud service provider, for example.

The legal requirements on a controller are more demanding than on a processor, and the penalties for a breach are greater. Therefore, "Secure by design" and "Privacy by design" solutions should be considered by the developer, technical team, administration, and legal needs. The system should be transparent and auditable, both to ensure trust and to ensure legal compliance.

5. WORKSHOP DISCUSSION AND OUTPUT



This section covers a short study to explore the possible acceptance and adoption of RAS over security and privacy concerns of the public. Before the survey was conducted with questionnaires consisting of ten questions, the questions were framed based on the workshop and panel discussion with experts in the field of AI, Cybersecurity, Robotics, Social and Health care, Law, Social Scientists including industrial experts. The workshop was conducted to study and discuss the robotic security and privacy issues under the UK-RAS pump priming project which was participated by academics and researchers from across eight different universities of the UK (Sheffield Hallam University, University of Manchester, Loughborough University, University of Nottingham, Nottingham Trent University, University of Glasgow, De-Montfort University, University of Sheffield) along with an Industrial partner IBM. During the workshop, a total of 28 participants were involved.

Figure 10, Figure 11, and Figure 12 are based on the data collated via Mentimeter during the workshop session moderated by The Care Machine Ltd at AWRC. During the discussion, Figure 10 highlights the key opportunities (such as robots for service and elderly care, acceptance and adoption, friendship, etc) for RAS in the future; Figure 11 represents the word cloud of some of the biggest concerns in RAS such as security, privacy, and trust. While Figure 12 reflects the points that are important to society in RAS adoption e.g., safety and safeguarding, access to personal data, cyberthreat prevention etc.

Using these questions derived from the workshop, responses from potential care robot users were collected and depicted in Figure 13 from one of the public engagements with a care robot at AWRC, Sheffield Hallam University. The survey was conducted with the public on two different occasions.

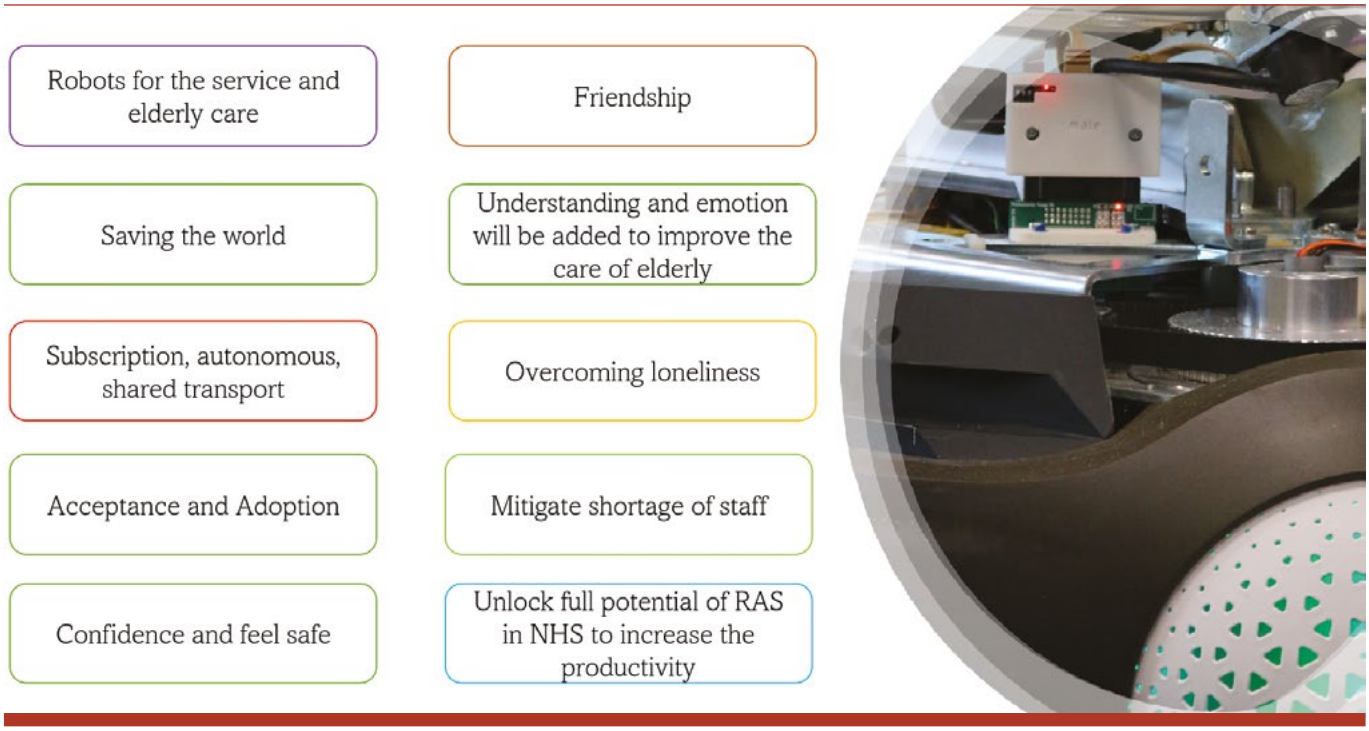


Figure 10:
Opportunities for RAS in the Future (Robot picture from AWRC, SHU, 2022)

Figure 11:
Biggest Concerns in RAS (Robot picture from AWRC, SHU, 2022)

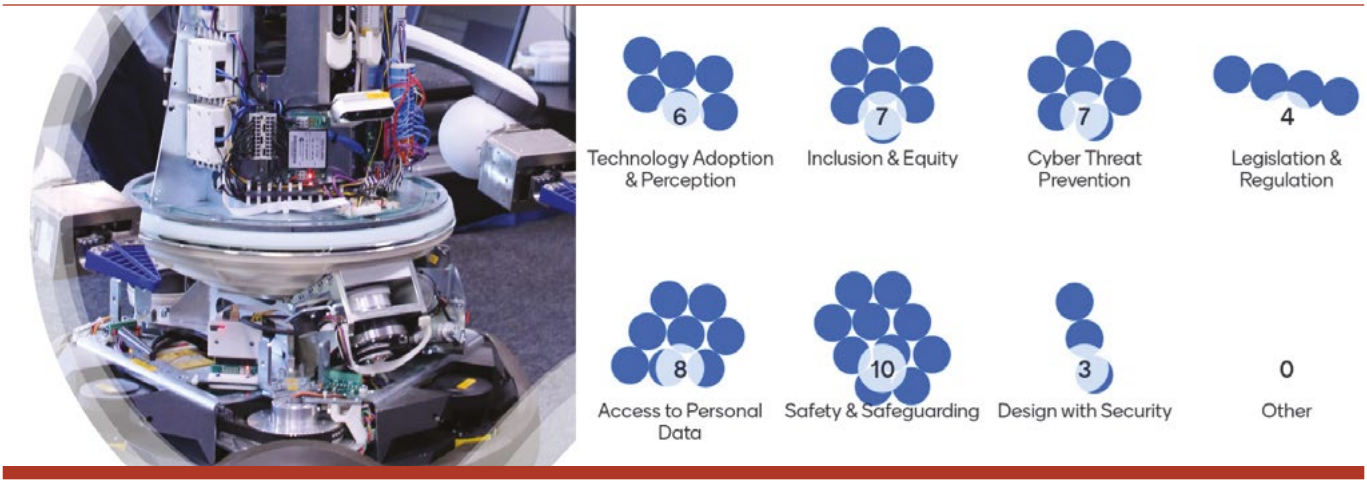


Figure 12:
Importance to Society in RAS Adoption (Robot picture from AWRC, SHU, 2022)

Figure 13:
Picture of a Public Engagement during Care-O-Bot Demo at AWRC, SHU, Sheffield, 2022.

5.1. SURVEY METHODOLOGY DURING PUBLIC ENGAGEMENTS

To understand and capture the importance of protecting the care RAS and its users' data from cyber threats, a survey was conducted with the participants from Darnall Wellbeing Community (A voluntary, community and social enterprise organisation), Sheffield, UK, and the Public Involvement in Research Group (the group that provides a platform to enable researchers to engage with and for the public) of the Advanced Wellbeing Research Centre (AWRC), Sheffield Hallam University and public of the city of Sheffield. The user study involved 30 potential public users (13 female and 18 male) between the age of 45 and 90 years. During the public engagement events, presentations and discussions were held with the participants about assistive care robots, which highlighted their importance and their usefulness in improving quality of life and supporting independent living. After the demo and a discussion session of each public engagement, a survey was then conducted using the questions highlighted earlier to capture their level of understanding and their perceived importance of security and user privacy issues in care RAS. No cybersecurity and AI experts were allowed to participate in this survey, so the views collected are solely based on general social perception and understanding of care RAS and the questions are highlighted in Appendix-A. Out of 30

participants, only 14/30 (46.66%) participants knew or used some form of an assistive system like Alexa, Siri, or any virtual assistant like Google, an automated telephone tree; the rest of the participants reported using very little or confess of not knowing about such automated systems.

So, the participants had a good spread across knowledge and skills of autonomous and assistive systems. Interestingly, only 8/30 (26.66%) had at least some knowledge about assistive robots and their ability to take care of older and disabled people.

5.2. FINDINGS OF THE SURVEY FROM PUBLIC ENGAGEMENTS

When it comes to preferences, in terms of receiving care from a RAS over a human, it was interesting to observe that the majority i.e., 23/30 (76.66%) of the participants prefer to receive at least some form of services from the former over the latter: this happens because they feel that the care robot can also be a companion and a protector which is willing to provide services round the clock without any exhaustion or frustration, unlike humans. The majority of the participants, i.e., 23/30 (76.66%) have at least some forms of reservation on how the care robot collects, processes, and stores the user's data and with whom it is shared. When it comes to the data generated between RAS and the user, an overwhelming 28/30 (93.33%) believe that the data should be transmitted securely, shared, processed, and stored securely. When it comes to user privacy, almost all the participants i.e., 29/30 (96.66%) believe that it should always be safeguarded and protected. It was interesting to observe that 23/30 (76.66%) feel that, unless RAS is secure, they may either use its services reluctantly or as little as possible, if not at all. This is a genuine concern that will be affecting the acceptance and adoption of RAS. In addition, 21/30 (70%) of the participants think that unless security and privacy issues are addressed, then the RAS cannot be trusted, or it will be trusted with very low confidence. In addition, all the participants i.e., 30/30 (100%) feel that for a safe adoption of RAS, this must be secured, and the user's privacy should be protected. It was also interesting to note that all the participants believe that they have concerns that care robots could increase their risks by making them a target for theft of property or data. Their perception could be right since care robots are expensive and hold sensitive, valuable user data. Generally, when the perception is negative or people are worried or concerned, acceptance and adoption are going to be affected. So, such transformative RAS technology adoption should not be hampered by concerns over security and privacy. Figure 14 presents some written feedback provided by the potential future RAS users regarding trust issues and other challenges in RAS adoption. As RAS deployment has become a reality in care sectors, the key highlighted issues and challenges need to be addressed to improve social acceptance and trust, otherwise users could become sceptical about this transforming technology.

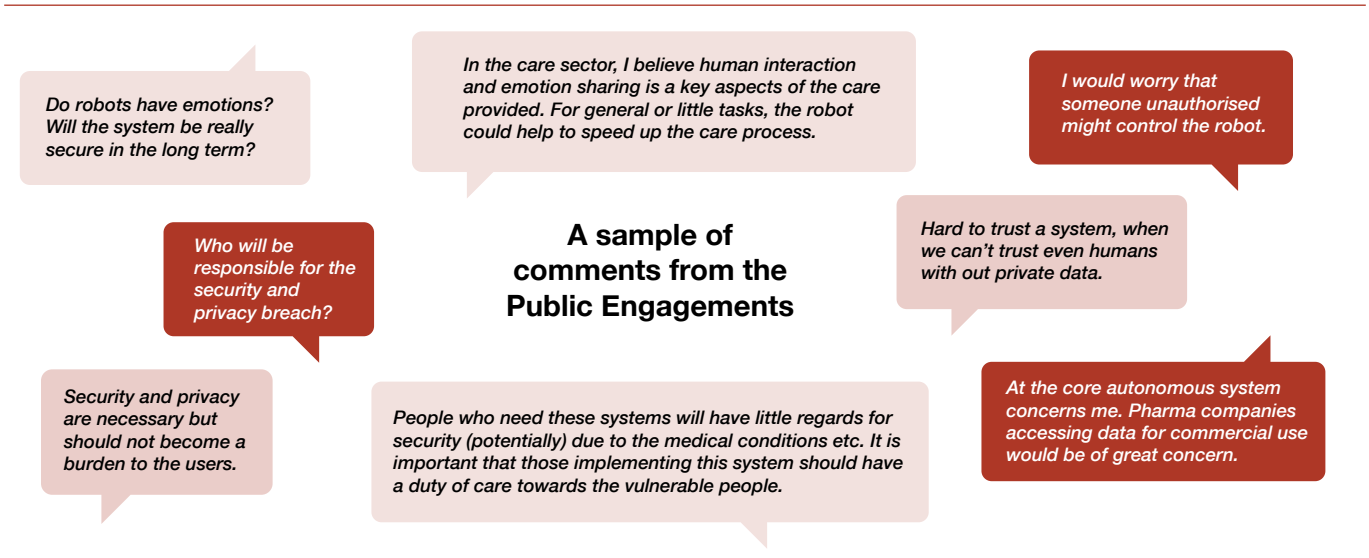


Figure 14:
Some Interesting Feedbacks about care RAS from Public Engagements, at AWRC, SHU, Sheffield, 2022.

6. CONCLUSION

RAS is a resource-hungry system in terms of computation, storage, and bandwidth requirements, especially when connected to cloud services or a network. Although incorporating security and privacy mechanisms will increase the RAS overhead, care RAS deals with sensitive data of the health and wellbeing of a user. Therefore, GDPR compliance is necessary. Moreover, without these mechanisms in place, RAS is vulnerable to being attacked, manipulated and weaponised by unauthorised control and malfunctioning the RAS' actions and functions, ultimately putting RAS services, the user, the user's data, and the user's privacy at risk. Security and privacy must be considered to ensure that the care RAS is safe for the users, resilient, and free of cyber risks, while also being acceptable and trustable for a high adoption rate. This positive perception of care RAS technology will encourage users to adopt it. However, adding security solutions can make the system more complex and affect its usability, especially for older or disabled users who need care support. Therefore, security and privacy-preserving mechanisms should not become a hurdle or burden for receiving RAS services, but rather easy to use, adopt, and trustable.

6.1. RECOMMENDATIONS

The following recommendations for the design, development and use of intrinsically secure RAS systems are made after analysing, observing, and receiving feedback from potential users, stakeholders, and subject experts.

1. Secure by Design: All the security mechanisms and techniques should be incorporated from the start of the design and the development of RAS. Moreover, intelligent threat analysis and techniques should also be incorporated within RAS to reduce or avoid any impact of cyber threats on the RAS network, RAS, RAS control system, its user, and the user's data.

2. Privacy by Design: Care RAS is multimodal in terms of interaction and engagement with the user, so, all its channels, its services, engagement or interaction, and the user's data should be protected from the start of the design to safeguard the user's privacy. In addition, the care RAS should be disciplined so that it should not collect, share, or leak any user's private data to any stakeholders or unauthorised individuals without the user's authorisation and consent. (Exceptions may apply e.g., when the user's life is at risk and the user cannot give consent, but non-ethical safe intervention is needed for the user's welfare)

3. Trust: The care RAS system should be transparent, auditable and traceable to ensure and maintain user confidence and safe adoption.

4. Scalability: A careful trade-off between the quality of the RAS service delivery and system overheads should be considered in designing and developing care RAS to ensure a real-time response.

5. Usability: The security and privacy safeguarding mechanisms should follow a user-centric approach to avoid becoming a barrier or burden.

6. Rules: New Government policies, laws, regulations, and compliances need to be developed for care RAS technology to avoid any user rights violations and safe adoption.

Although RAS is already gaining popularity, building user trust, and promoting the adoption of RAS will also depend on the incorporation of robust mechanisms to safeguard its integrity, increase its reliability, and protect its users' privacy. Therefore, incorporating security and privacy features into the design of RAS will enhance their trustworthiness and promote their acceptance in various industries, including healthcare. In conclusion, we recommend that it is crucial to prioritise the integration of these safeguarding techniques to ensure that RAS meet the highest standards of security, privacy, reliability, and data protection regulations.

7. REFERENCES

[1] United Nations; Department of Economic and Social Affairs; Population Division. World Population Prospects; Office of the Director, Population Division, United Nations, 2 United Nations Plaza, Room DC2-1950: New York, NY, USA, 2019.

[2] Market Analysis Report: Robotic Nurse Assistant Market Size, Share & Trends Analysis Report By Product Type (Independence Support Robots, Daily Care & Transportation Robots), By End-use, By Region, And Segment Forecasts, 2022 – 2030, Report ID: GVR-3-68038-962-3, Pages: 80, Format: Electronic (PDF), Historical Range: 2016 – 2020. https://www.grandviewresearch.com/industry-analysis/robotic-nurse-assistant-market

[3] Postnote, Houses of Parliament, Parliamentary office of Science and Technology, 2018. Robotics in Social Care. Number 519. https://post.parliament.uk/research-briefings/post-pn-0591/

[4] Kyrarini, M., Lygerakis, F., Rajavenkatanarayanan, A., Sevastopoulos, C., Nambiappan, H. R., Chaitanya, K. K., Babu, A. R., et al. (2021). A Survey of Robots in Healthcare. Technologies, 9(1), 8. MDPI AG. Retrieved from http://dx.doi.org/10.3390/technologies9010008

[5] Di Nuovo, A., Broz, F., Wang, N., Belpaeme, T., Cangelosi, A., Jones, R., Esposito, R., Cavallo, F., Dario, P.: (2018). The multi-modal interface of Robot-Era multi-robot services tailored for the older . Intelligent Service Robotics. 11, 109–126

[6] Di Nuovo, A.; Varrasi, S.; Lucas, A.; Conti, D.; McNamara, J.; Soranzo, A. (2019a) Assessment of Cognitive skills via Human-robot Interaction and Cloud Computing. J. Bionic Eng., 16, 526–539.

[7] Cavallo, F., Esposito, R., Limosani, R., Manzi, A., Bevilacqua, R., Felici, E., Di Nuovo, A., Cangelosi, A., Lattanzio, F., Dario, P. (2018): Robotic services acceptance in smart environments with older adults: user satisfaction and acceptability study. Journal of medical Internet research. 20, e264 (2018).

[8] Local Government Association, 2018. Hampshire County Council: pushing the boundaries by using Amazon Echo. https://www.local.gov.uk/hampshire-county-council-pushing-boundaries-using-amazon-echo (accessed on 20/11/2022)

[9] Carehome.co.uk, 2018. Care South introduce robotic therapy pets with positive results https://www.carehome.co.uk/news/article.cfm/id/1597708/care-south-introduce-robotic-therapy-pets-with-positive-results (accessed on 22/11/2022)

[10] IBM security, X-force Threat Intelligence Index, 2023 Report. https://www.ibm.com/downloads/cas/DB4GL8YM

[11] IBM security, X-force Threat Intelligence Index, 2022 Report. https://www.ibm.com/downloads/cas/ADLMYLAZ

[12] IBM Security, Services Cyber Security Intelligence Index (2014), IBM Global Technology Services Managed Security Services, Research Report.

[13] Age UK, 2019. Older person becomes victim of fraud every 40 seconds. https://www.ageuk.org.uk/latest-press/articles/2019/july/older-person-becomes-fraud-victim-every-40-seconds/ (Published on 31 July 2019, accessed on 13/11/2022).

[14] Golinelli, D.; Boetto, E.; Carullo, G.; Nuzzolese, A.G.; Landini, M.P.; Fantini, M.P. Adoption of digital technologies in health care during the COVID-19 pandemic: Systematic review of early scientific literature. J. Med. Internet Res. 2020, 22, e22280.

[15] Anthony Jnr, B. Implications of telehealth and digital care solutions during COVID-19 pandemic: A qualitative literature review. Inf. Health Soc. Care. 2021, 46, 68–83. https://doi.org/10.1080/17538157.2020.1839467.

[16] Camp, N., Lewis, M., Hunter, K., Johnston, J., Zecca, M., Di Nuovo, A. and Magistro, D., Technology used to recognize activities of daily living in community-dwelling older adults. Int. J. Environ. Res. Public Health 2021, 18, 163.

[17] Getson, C. and Nejat, G., Socially Assistive Robots Helping Older Adults through the Pandemic and Life after COVID-19. Robotics 2021, 10, 106.

[18] United Nations; Department of Economic and Social Affairs; Population Division. World Population Prospects; Office of the Director, Population Division, United Nations, 2 United Nations Plaza, Room DC2-1950, New York, NY 10017, USA, 2019.

[19] Pu, L.; Moyle, W.; Jones, C.; Todorovic, M. The Effectiveness of Social Robots for Older Adults: A Systematic Review and MetaAnalysis of Randomized Controlled Studies. Gerontologist 2019, 59, e37–e51. https://doi.org/10.1093/geront/gny046.

[20] Allaban, A.A.; Wang, M.; Padır, T. A Systematic Review of Robotics Research in Support of In-Home Care for Older Adults. Information 2020, 11, 75. https://doi.org/10.3390/info11020075.

[21] Bedaf, S.; Gelderblom, G.J.; De Witte, L. Overview and categorization of robots supporting independent living of older people: What activities do they support and how far have they developed. Assist. Technol. 2015, 27, 88–100.

[22] Beuscher, L.M.; Fan, J.; Sarkar, N.; Dietrich, M.S.; Newhouse, P.A.; Miller, K.F.; Mion, L.C. Socially assistive robots: Measuring older adults' perceptions. J. Gerontol. Nurs. 2017, 43, 35–43.

[23] Conti, D.; Di Nuovo, S.; Di Nuovo, A. A brief review of robotics technologies to support social interventions for older users. Hum. Cent. Intell. Syst. Smart Innovation, Systems and Technologies, (189) 2020, pp.221–232.

[24] Cavallo, F.; Esposito, R.; Limosani, R.; Manzi, A.; Bevilacqua, R.; Felici, E.; Di Nuovo, A.; Cangelosi, A.; Lattanzio, F.; Dario, P. Robotic services acceptance in smart environments with older adults: User satisfaction and acceptability study. J. Med. Internet Res. 2018, 20, e264.

[25] Frennert, S.; Ö stlund, B. Seven matters of concern of social robots and older people. Int. J. Soc. Robot. 2014, 6, 299–310.

[26] Sharkey, A.; Sharkey, N. We need to talk about deception in social robotics! Ethics Inf. Technol. 2021, 23, 309–16.

[27] Char, D.S.; Shah, N.H.; Magnus, D. Implementing machine learning in health care—addressing ethical challenges. New Engl. J. Med. 2018, 378, 981.

[28] May, R.; Denecke, K. Security, privacy, and healthcare-related conversational agents: A scoping review. Inform. Health Soc. Care. 2021, 1–17. https://doi.org/10.1080/17538157.2021.1983578. Epub ahead of print. PMID: 34617857.

[29] Wachter, S.; Mittelstadt, B.; Floridi, L. Transparent, explainable, and accountable AI for robotics. Sci. Robot. 2017, 2, eaan6080. https://doi.org/10.1126/scirobotics.aan6080.

[30] Pilkington, M. Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations; Xavier, F., Zhegu, O.M., Eds.; Edward Elgar Publishing: London, UK, 2015; pp. 1–39.

[31] Peck, M.E. Blockchains: How they work and why they'll change the world. IEEE Spectr. 2017, 54, 26–35. https://doi.org/10.1109/MSPEC.2017.8048836.

[32] Samuel D. Warren and Louis D. Brandeis. "The right to privacy". In: Harvard Law Review 4.5 (1890), pp. 193–220.

[33] Ferdinand David Schoeman. Privacy and Social Freedom. Cambridge University Press, 1992.

[34] Grazia Cecere, Fabrice [Le Guel], and Nicolas Soulié. "Perceived Internet privacy concerns on social networks in Europe". In: Technological Forecasting and Social Change 96 (2015), pp. 277–287. issn: 0040-1625. doi: https://doi.org/10.1016/j. techfore.2015.01.021.

[35] Alan F. Westin. "Privacy and Freedom". In: Social Work 13.4 (Oct. 1978), pp. 114– 115. issn: 0037-8046. doi: 10.1093/sw/13.4.114-a.

[36] Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 1st Oct 2022)

[37] Marchang, J. and Di Nuovo, A., 2022. Assistive multimodal robotic system (AMRSys): security and privacy issues, challenges, and possible solutions. Applied Sciences, 12(4), p.2174.

[38] Bayreuther, S., Jacob, F., Grotz, M., Kartmann, R., Peller-Konrad, F., Paus, F., Hartenstein, H. and Asfour, T., 2022, June. BlueSky: Combining Task Planning and Activity-Centric Access Control for Assistive Humanoid Robots. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies (pp. 185-194).

[39] Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S. and Schartner, P., 2017. Security for the robot operating system. Robotics and Autonomous Systems, 98, pp.192-203.

[40] ICO, 2021. Introduction to Anonymisation. https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

[41] European Union Agency for Cybersecurity, 2019. Pseudonymisation techniques and best practices. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

[42] ICO, 2019. Guide to Data Protection. https://ico.org.uk/for-organisations/guide-to-data-protection/

8. APPENDIX - A

The questions used in the survey are listed in the following table.

Q1	Have you ever interacted or engaged with any kind of robots including Alexa, Siri, or any virtual assistance like google, automated telephone tree etc. (They are all some kind of assistive robots)?
Q2	Do you know robots can be used to take care of the people who are elderly and disabled, to improve quality of life (reduce loneliness, be a companion, be a Carer, monitor the user's health and wellbeing, monitor the user's activity and provide services as per user's preferences)?
Q3	Overall, human carers are expensive, their availability is limited, they often get exhausted and frustrated. Some carers can even take advantage of their vulnerable patients. On the other hand, care robots will be able to assist the users 24/7, with no risk of harm or exhaustion or frustration, and no risk of fraud or abuse. In fact, the care robot will be your companion and protector, as well as carer, nurse and doctor. A robot will not react negatively to your emotions, and it will never hurt or harm you. Given such circumstances, would you prefer to use a care robot to support independent living over a human carer?
Q4	A care robot would be with you, sees you, monitors you and your activity, it collects all the data about you and the activities which are personal and sensitive in nature. How much would you care how the robot collects the data, processes the data (where – local or cloud?), stores the data (where - local or cloud?), and shares the data (with whom?), because otherwise your privacy could be or will be compromised and it may even lead to fraud and abuse?
Q5	Do you think all the user data related to interaction with the care robot and the user should be securely transmitted, securely shared, securely processed, securely stored?
Q6	Do you think, the privacy of the user should be safeguarded and always protected, and any sensitive information should not be made visible to any unauthorised or unintended people or inappropriate users without the authorisation and approval of the owner (Note that GDPR doesn't cover the aspect of privacy related to the inappropriate situations or scenarios e.g., in presence of children or different culture or race that could affect an aspect of racism rather it focuses on unauthorised users)? NOTE: Existing legal protection to safeguard users of RAS is not clear.
Q7	If the care robot is not secured, unauthorised users can access user information, and can control the robot, misguide, and misdirect the robot, and even weaponize the robot. If that is the case, will you still use the robot because it is useful e.g., like our phone (Our voice and Text messages are not secure, but we use it every day and it has become part of our lives).
Q8	If the robot's interaction, engagement, mode, and level of access are not guaranteeing the security and privacy of the user's, will you TRUST the robots?
Q9	Security and privacy are key to users trusting care robots and eventually adopting their use with confidence.
Q10	Using a care robot could increase the personal risk for the patient by making them a target for theft of either the robot or the data it contains. Would you have concerns about such cases?

> Although RAS is already gaining popularity, building user trust, and promoting the adoption of RAS will also depend on the incorporation of robust mechanisms to safeguard its integrity, increase its reliability, and protect its users' privacy.

UK-RAS NETWORK
ROBOTICS & AUTONOMOUS SYSTEMS

www.ukras.org.uk