Assistive multimodal robotic system (AMRSys): security and privacy issues, challenges, and possible solutions

MARCHANG, Jims <http://orcid.org/0000-0002-3700-6671> and NUOVO, Alessandro Di <http://orcid.org/0000-0003-2677-2650>

applied sciences

MDPI

Article

Assistive Multimodal Robotic System (AMRSys): Security and Privacy Issues, Challenges, and Possible Solutions

Jims Marchang * and Alessandro Di Nuovo

Computing Department & Advanced Wellbeing Research Centre (AWRC), Sheffield Hallam University, Sheffield S1 1WB, UK; a.dinuovo@shu.ac.uk
* Correspondence: jims.marchang@shu.ac.uk

Abstract: Assistive robotic systems could be a suitable solution to support a variety of health and care services, help independent living, and even simulate affection, to reduce loneliness. However, adoption is limited by several issues, as well as user concerns about ethics, data security, and privacy. Other than the common threats related to internet connectivity, personal robotic systems have advanced interaction possibilities, such as audio, video, touch, and gestures, which could be exploited to gain access to private data that are stored in the robot. Therefore, novel, safer methods of interaction should be designed to safeguard users' privacy. To solicit further research on secure and private multimodal interaction, this article presents a thorough study of the state-of-the-art literature on data security and user privacy in interactive social robotic systems for health and care. In our study, we focus on social robotics to assist older people, which is a global challenge that is receiving a great deal of attention from the robotics and social care communities. This application will have a significant positive impact on the economy and society, but poses various security and privacy issues. This article analyses the key vulnerable areas where data leakage could occur during a multimodal interaction with a personal assistive robotic system. Thus, blockchain with a resource-aware framework, along with a continuous multifactor authentication mechanism, are envisaged as a potential solution for making such systems secure by design; therefore, increasing trust, acceptability, and adoption. Among the key cybersecurity research challenges, it is crucial to create an intelligent mechanism that autonomously determines the right trade-off between continuous user prompts and system usability, according to data types and personal preferences.

Keywords: assistive technology; multimodal interaction; social robotics; privacy; security

Citation: Marchang, J.; Nuovo, A.D. Assistive Multimodal Robotic System (AMRSys): Security and Privacy Issues, Challenges, and Possible Solutions. *Appl. Sci.* **2022**, *12*, 2174. https://doi.org/10.3390/app12042174

Academic Editor: Mourad Oussalah

Received: 24 December 2021
Accepted: 14 February 2022
Published: 19 February 2022

1. Introduction

Technology has transformed the health and care system, to address the issues of shortages in manpower and to improve services for patients. Digital solutions are increasingly adopted to facilitate access to the required services, especially during the pandemic, as described in [1–4]. For instance, a growing body of research shows that social robotic systems can well address the physical, cognitive, and social needs of older people [5–7]. Assistive robots with social interaction capability, i.e., socially assistive robotics, have great potential to support and augment healthcare providers in helping physically, cognitively, and supporting older people socially [8,9]. For a successful implementation of socially assistive robots, it is critical that older people accept and respond to the design, ways of communication, and interaction [10]. For these reasons, we focus this study on the application of social robotics to assist older people, which represent the most promising and advanced application so far. However, the findings that we will present can be generalised to other socially assistive robotics applications, such as the care of people with disabilities.

Nowadays, governments from all around the world are in the midst of a growing crisis in the demand for assistance of older people and the shortage of health support workers. Assistive robotic systems offer an innovative solution to support care services and provision of human-like affection [11]. However, this technology has several issues and concerns pertaining to its acceptance with respect to ethics [12–14]. In addition, intelligent social robots that implement conversational agents have issues pertaining to users' data privacy [15], which also affect the users' physical, social bonding, psychology, and social privacy [16]. Moreover, in general, even simple patient monitoring systems and devices, need to be secure and preserve users' privacy [17]; therefore, so much more is required for an effective assistive robotic system.

To show the global dimension of the issue, Table 1 provides the ageing population distribution of the world, which will be more than doubled in the next thirty years; thus, the current problems will be amplified. As per the United Nations, Department of Economic and Social Affairs, Population Division (2019) [18], in Europe and Northern America many older people prefer to live independently (unlike other subcontinents such as Asia, Africa, and Latin America, where the older prefer to live with their children) and this is where we predict that socially assistive robotic systems could become most popular, to support and provide necessary assistance to promote independent healthy living.

Table 1. Source: United Nations, Department of Economic and Social Affairs, Population Division (2019). World Population Prospects 2019.

Region	Number of Persons Aged 65 or Over in 2019 (millions)	Number of Persons Aged 65 or Over in 2050 (millions)	Percentage Change between 2019 and 2050
World	702.9	1548.9	120
Sub-Saharan Africa	31.9	101.4	218
Northern Africa and Western Asia	29.4	95.8	226
Central and Southern Asia	119.0	328.1	176
Eastern and South-Eastern Asia	260.6	572.5	120
Latin America and the Caribbean	56.4	144.6	156
Australia and New Zealand	4.80	8.80	84
Oceania, excluding Australia and New Zealand	0.50	1.50	190
Europe and Northern America	200.4	296.2	48

Given all the required functionalities, a human-like appearance and the technical ability to provide required services may not be sufficient for acceptance and use of multimodal social robotics among health and care digital assistants. One of the other biggest questions is *Can we trust the machines?* Indeed, level of trust has a significant impact on how much users comply with artificial agents [19], which is critical in medicine, as low compliance with prescriptions can cause adverse outcomes for patients' health.

This article focuses on social and care assistive multimodal robots' security and privacy issues. Such a robotic system interacts with the user to learn the user's preferences, with the aim of providing a better service, and the user or any authorised users should be able to interact with the robotic system locally or remotely. In the process, this poses several unanswered questions pertaining to users' privacy and data security: What if the input data is manipulated? What if the stored data is either visible to, or corrupted or tampered with by an unauthorised user? What if the sensor data is fraudulent? What if the robot is accessed by unauthorised users? What if the robot and the sensory devices are hijacked by hackers? If connected remotely, how to approve users, control access, and limit their rights, and how security keys are managed, approved, and authorised. What about the user's privacy? Is the user's data leaked during communication and interaction unintentionally to unauthorised users? Where is the user's data stored and managed?

What if malware is running and controlling the system? What if a man-in-middle is accessing and controlling the robot? Thus, apart from acceptance and functionality for the robotic system, security and privacy preservation is important, so that it is safe to adopt. In addition, transparency of the robot's decision making is equally critical, so that the user knows exactly when, what, and why the decisions are taken by the robotic system, to gain the user's trust. Therefore, this article focuses on the transparency, privacy, and security issues of the robot, its user, its sensors, and its data. In order to address the transparency challenges of the robot, private permission-based blockchain technology is a potential solution for incorporating visibility and traceability to the authorised users. However, designing a scalable and energy-efficient blockchain framework is a research domain to explore, as blockchain is resource hungry and computation-intensive in nature. On the other hand, the robot's engagement should be real-time and computation overheads should not harm the robotics' real-time performance. The following sections cover the types of robots; detailed analysis of the state-of-the-art literature; and an in-depth study of transparency, security, and privacy requirements; as well as issues and challenges in a multimodal robotic system; followed by prospective solutions to make a system secure by design. The examples given in the following sections were selected based on their significance to the problem that we are analysing.

2. Types of Robots

Artificial Intelligence (AI) has transformed the way humans adapt robotic systems. It is also now used for performing various activities in the social domain, other than industrial processes. There are different categories of robots, depending on the requirements and their use [20,21]; they can be broadly classified as shown in Figure 1. Among all forms of robotic interaction, medical-related robots need the highest form of device and data protection, because they deal directly or indirectly with humans' health and wellbeing. In the social and care category using assistive robots, safeguarding user's privacy is as important as securing robots' data, storage, access, communication channels, protection of data sources (sensors) from tampering and malfunctioning, due to bugs and viruses or malware, etc. However, securing and preserving users' privacy in any assistive multimodal robotic system (AMRSys) is very challenging, because of the multiple channels and varying means of interacting and communicating with the user. The rest of this article will focus on assistive multimodal robotic security and privacy-preserving mechanisms and techniques to enhance trust and increase adoption among users.

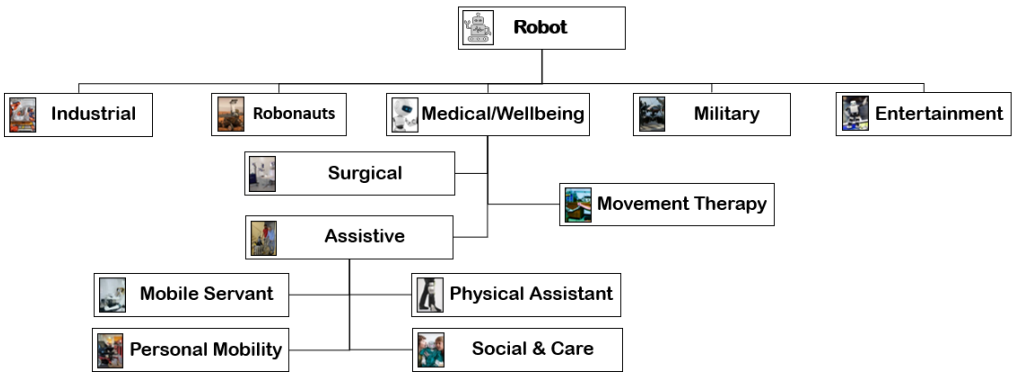

Figure 1. Different Types of Robotic Systems.

3. Background Study of Assistive Multimodal Robots

An ageing population, where older people prefer to live independently and where there is a shortage of care providers, leads to the need and popularity of assistive robotic systems as a solution. They have the potential to support disabled and older people in overcoming barriers and to increase independence, as highlighted in [22]. The authors of [23] conducted a systematic study on the impact of a socially assistive robotic system in a care system of older people and found the importance and the positive impact it brings to their lives. Social isolation is one of the key reasons for the development of dementia among older people, and an engaging experience with a social robot could improve their remembering of experiences, according to the authors of [24]. The analysis found that even governments encourage ageing at home to alleviate the cost of aged care facilities. Therefore, it is critical to design a user-centric care system, to satisfy and embed the users' needs in the assistive robotic system, so that the multimodal interfaces can recognize and interpret speech, gesture, gaze, movement patterns, and other complex natural behaviours, which may not be under the direct control of the conscious mind, as researched by the authors of [25]. Due to the computation limitations of current robotic systems, the requirement to experience a human-like service interaction with a robot may be hard to achieve; therefore, new approaches such as cloud computing for processing and storage could be a solution, while web-based interfaces for easy and flexible interaction could be an alternative. Thus, a user-centric design with a web-based multimodal user interface tailored to older users of futuristic multi-robot services was designed in [26]. The authors of [27] conducted an experimental validation of a robotic system for cognitive assessment via human–robot interaction that integrates a social robot with AI cloud computing. The psychological and behavioural measures allow computing systems to integrate user interaction experience by understanding the mental load and capacity. Multimodal coordination and behavioural measurements help in understanding the user and their activities, as described in [28]. The robot administers and records a set of multimodal interactions to engage with an understanding of the cognitive abilities of the user. Robotic scientists aim to integrate multiple sensors to promote multimodal interaction and find ways to make the robot productive and supportive in solving real-life human–robot interaction problems. In the process, the authors of [29] worked on detecting, tracking, and recognising techniques by using object weights which is inspired by computer vision techniques. It can even recognize content through a mix of inference and combinatorial search techniques. Other processes such as fuzzification in combination with dynamic multimodal sensor communication improve the probability of anomaly detection, as highlighted in [30]; while the work of [31] designed an active multimodal sensor to recognize, track, and incorporate the visibility of an infrared unit with a hyperspectral sensor, which could all but eliminate ambiguous recognition. Other authors, such as in [32], addressed simultaneous tracking and recognition of people within the robot sensing range and integrated with leg and face detection. To improve person recognition by social robots, a novel brain-inspired multimodal perceptual system was designed by the authors of [33], using a spiking neural network to integrate face, body features, and voice data in order to recognize a person in various social human–robotic interaction scenarios. Other researchers in [34] focused on adopting mixed reality for human–robotic interactions, in which humans control and coordinate the co-located robots using a see-through head-mounted display unit. This improved the security, acceptability, and predictability when conducting pick and place task.

A human robotic system faces the challenges of disharmony, which results in inefficient communication; therefore, multimodal emotional recognition is vital to minimize dullness during interaction and to address the need to increase the ability to understand empathy, as researched by [35]. Controlling the robot is important, and they can also be controlled by commands generated by application software, which works in an asynchronous fashion, as proposed in [36]. Some other robots can recognize hand gestures using

multimodal data fusion and a multiscale parallel convolution neural network. The accuracy and reliability of gesture recognition is high, as elaborated in [37]. There are robotic systems that focus on multimodal interaction to aid and support during walking, for people struggling and suffering from locomotion issues, as designed by [38]. Such robots aim to ensure safety, intuitiveness, and ergonomics. There are other interesting systems that track attention using a multisensory system in a multimodal environment, which helps in tracking the engagement of the user with the system [39]. A robotic system needs to comply with requirements, regulations, and instructions, to make it responsible and comply with the ethical considerations of the user requirements in home settings; unlike industrial robots that could put at risk and harm users because of a lack of understanding by and of the user [40]. To make it lifelike and realistic during engagement, it is important to understand human pose recovery and behavioural analysis, so that the system can deal with changes in appearance due to cloth, background, artefacts, illumination etc., and with knowledge of the articulated nature of the human body, as described in [41].

To enhance the performance of a robotic system, integration of the IoT is vital, and the implication and philosophy of the integration of IoT with robots, called the Internet of Robotic Things, is elaborated in [42]. The authors of [43,44] explore the integration of a robotic system with IoT technology, because this will advance the abilities and capabilities for creating innovative services. There is also potential for integration of a robot via a web called the Web of Things (WoT), to enhance its usability and performance, as explained in [45]. Even if a robot is functional in all aspects pertaining to the needs and service requirements of the user, without mechanisms to safeguard the privacy and security of the robot, it will not be adoptable or acceptable. Therefore, the applications, data collection, generation, storage, devices, and sensors with which it interacts need to be safeguarded from data leakage and system malfunctioning or damage, and it should be made mandatory to incorporate state-of-the-art security mechanisms. The authors of [46] conducted a thorough investigation of several existing robots from multiple vendors to check vulnerabilities, and it was found that there were many critical cybersecurity issues, including insecure communication, weak default configurations, and weak authentication and authorisation schemes identified in robot operating systems (ROS). A robotic system OS could be infected by malware and virus, and since assistive robotic systems are multimodal in nature, even when malware infects the system, a multimodal malware detection method is required, just like the ones that are designed for a multimodal smart android system [47]. It is vital to make the system transparent, accountable, and explainable and to have precise regulations and methods to certify, explain, be auditable, and be scrutable [48]. To ensure communication security, maintain data integrity, and have tamperproof, transparent storage security and traceability, blockchain technology, as described in [49,50], can be adopted in an assistive robotic system. However, blockchain technology is resource hungry, so it would be a daunting to integrate. Similarly, it can also be integrated with the IoT network and the robotic system, to ensure reliability, resilience, and susceptibility, as proposed in [51].

Last but not the least, apart from human-like functionalities and data security, it is very important to protect users' privacy, otherwise it would be hard to trust the system and the adoption rate would be adversely affected. It is vital to assess the implications of privacy in the integration and associations with domestic robotic systems. This is important because it is the user's right to protect and safeguard their privacy, and the robot should not expose or leak user's information, in order to be aligned with ethical requirements [52]. The data protection acts of the GDPR, human rights, and other regulations cannot protect users' privacy unless mechanisms and techniques are incorporated into the robotic system itself. That something is not allowed, does not mean this will not be violated or will not be committed or will not be broken. This is the reason why privacy and security in multimodal user interfaces of social media applications are vital, even for social media [53], and the ways and means of leaking information are even more apparent in a multimodal robotic platform, with damaging and even life-threatening results, due to

leakage of personal information or hackers controlling the robot. Therefore, it is critical to protect and safeguard users' privacy and the security of multimodal robots, as well as the interaction between the user and the robots. This is one of the reasons why even connected vehicles need to preserve its privacy when a multimodal system is used, so invoking authentication process is a key requirement to safeguard and protect the system, as described in [54].

There is no known literature work that discusses in-depth multimodal assistive robotic security and privacy concerns and their challenges and solutions, apart from a few articles that discussed the security vulnerabilities of some robotic systems and possible attacks in general. The key contribution of this article, apart from the state-of-the-art literature study, is that it highlights the main cybersecurity issues and challenges in a multimodal assistive robotic system and proposes research directions for addressing these challenges, as well as design frameworks to incorporate innovative security mechanisms to guarantee safe and secure adoption of the technology. Table 2 highlights the system security requirements of a multimodal robotic system; as well as the motivations, current state of the research, in terms of security and privacy issues, in a multimodal robotic system, and highlights prospective solutions.

Table 2. Security and Privacy Requirements and Prospective Solution Directions [46,49–51,55–61,62–64,65].

Requirements	Motivation	Current State	Possible Solution
Transparency	User would know what, why, and when actions are taken by the robot.	No known blockchain solutions exist for a multimodal robotic system, but a detailed survey about blockchain solutions in robotics is highlighted in [55]. There are lots of blockchain solutions in different applications, as provided by different authors in [49–51,57,59–61]. It could also be applied for a security solution in a multimodal robotic system.	A private blockchain with permission based access control mechanism is a potential solution. So that only authorised users can access the data, but it would be designed in such a way that the consensus technique and storage does not affect the blockchain network performance. The design would consider the block storage mechanism, data trasmission rate, computation power requirement for block update, and validation process and participation of nodes during consensus to improve efficiency and reduce overheads.
Security and Privacy Threat Modelling Framework	To understand methods and means of attack and to protect user's data and privacy.	The authors of [46] explored the vulnerabilities of robots, but no security framework or solution was designed.	The threat model differs depending on the environment, presence of users, local or remote access, and the presence of intruders or unauthorised users. Therefore, secure frameworks would be develeoped in such a way that the robot communicates with the users if and only if the user's privacy is protected and the enviroment is safe and channel secure.
Channel Security	Avoid data leakage	There are no known solutions for an interative or multimodal robotic system because audible conversation between the user and robot cannot be encrypted. Transmission using technology such as a tablet, internet, phone etc. can be secured by using any standard data encryption techniques such as AES and RSA; but note that DES is vulnerable and not secure. DES	User and assistive robot communication should be secured. However, it would be impoossible to secure all the channels, e.g., the verbal conversation, signals, and signs in presence of other users. Therefore, the robot should know what to do and what to say and when to say it, or when to provide the service (in other words teaching the robot to behave in such scenario may be the best solution to secure data and preserve user's privacy). If technology is used to communicate with assistive multimodal robots then this can be secured easily using any standard encryption

		has been depreciated by the NIST since 2017.	techniques, but the method used should not degrade the robot's performance and response time.
Data Integrity and Avalability	To avoid non-repudiation and tampering. Detect and protect from attacks to increase data availability etc.	Secure standard hashing algorithms should be used like SHA2, SHA3 etc. Because hashing like SHA0, MD4, MD5 are no longer secure, so it should be avoided [56], even SHA1 is no longer secure, since hash collision attack was found by Google (https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html, accessed 12/01/22) recently. Authors of [58] conduct a systematic review paper on robotic attacks, counter-measures and recommendations but not related to multimodal security system.	No new mechsnisms for data integrity would be developed, but the most effective mechanisms would be explored and incorporated in a blockchain solution. A novel approach of an efficient integrity detecting technique would be developed within a merkle tree of a blockchain system, so that any attempt at tampering is self-healing within a node. This would avoid invoking other nodes or devices for approval or concensus when changes within a block take place after it is created and validated. This approach would revert any changes safely to the original state of the block. Such an approach will improve the effiency of the lockchain system and reduce energy consumption and computation power.
Unintended, Inappropriate and Intruder	To protect user's data and safeguard user's privacy.	There is no known solution for multimodal assistive robotic system. Even the existing interactive Alexa system doesn't differentiate the users be it authorised user or unauthorised users as long as the wake up code word is known. If wake up code word is considered as an authentication then probably this is the weakest known authentication technique. The Alexa system doesn't successfully differentate between the sounds of "Alixa, Alexsha, Alisha".	The interactive robotic system should have strong access control mechanisms to uniquely identify authentic users, and it should be aware of the presence of others and provide the services to the user only at an appropriate time and place. It should also know what is appropriate, e.g., an interactive system such as Alexa doe not know what is age appropriate; but it is very important to know what information to share with whom and whose presence is key to safeguard the user's privacy and protect against data leakage. Protecting against intruders will involve monitoring the activity and requests from users. Intrusion detection and prevention mechanisms should be in place to safeguard against intruders. To avoid man-in-middle attacks during remote connection, a safe and secure IP security technique should be applied.
Access Control (Identification, authorisation, access rights etc)	So that only authentic users and authorised users have an access and have a mechanism to limit the access rights.	The existing access control and authentication techniques [62–64] will not be appropriate in most of cases, because assistive multimodal robotic systems are to be adopted by older, disabled, or physically challenged people. Moreover, without continuous authentication, the data and the privacy will be leaked easily because of the nature of the assistive robotic system's multimodality. Using heart signals could be a potential solution to ensure a continuous	Using traditional password-based, token, or passphrase authentication may be challenging to use for older people and disabled individuals. It would also be hard to adopt if biometric authentications such as a fingerprint is used. Moroever, one time authentication would leave the robotic system open from attacks, as an Alexa waiting for a request once it wakes up. Therefore, a continuous and a seamless authentication mechnism needs to be developed so that the older, disabled, or physically challenged individuals can use the system without any worries about leaving the system open for attacks. In addition, the continuous authentication process should use no, or minimal, user knowledge or remembering capacity, so that its seamless and easy to adopt. Moreover, the

		and seamless authentication [65].	input factors for the authentication should be multi-factor, accurate, reliable, and consistent, so that they d not fail when the user's heath condition changes, e.g., sick or not well.
Network and Storage Security	So that remote access, storage do not leak user data.	During the remote access, available standard IPSec security mechanisms would be adopted, and to protect the robotic system, a proxy system would be in place. In addition, storage security e.g., encryption is available; however, there is no mechanism to protect from tampering, deletion, etc., by attackers or unintentional actions by authentic users, etc.	A private permission based blockchain system would be designed. It would be designed in such a way that the blocks will not hold the data, but only parameters necessary to detect and identify any changes to the actual data, so that the resource hungry blockchain does not degrate the robotic performance. Moreover, the storage framework should not lead to a single point failure either.
Scalability, user and system constraints	So that the assistive robotic system can serve multiple users, performance does not degrade, overheads are low, and reponse time is sensitive.	Blockchains are resource hungry in nature, but Cardano (https://whitepaper.io/coin/cardano, accessed 12/01/22) and Decentraland (https://decentraland.org/, accessed 12/01/22)-based solutions for NFT may be the way forward, to make the blockchain network light and efficient.	This approach would adopt existing techniques, but methods have to be developed in such a way that the system is easily adoptable and usable. It should also be easy to integrate with the assistive robotic system, so that the overheads do not degrade the response time and performance of the robotic system. Moroever, the data should be stored encrypted, and visibility should be controlled based on the needs and rights of the users and the third party service providers, such as the engineer, nurse, doctors etc.

A detailed study on the contributions of this article are highlighted below, forming the remainder of the article in different sections, i.e., the need for transparency of a multi-modal robotic system is described in Section 4, and Section 5 discusses security and privacy threat modelling for AMRSys. Security measurements for safeguarding and protecting users' data in a AMRSys are covered in Sections 6, and Section 7 covers security and privacy challenges and their limitations in AMRSys. In Section 8, a cyber-attack assessment on AMRSys is conducted. Then, Section 9 provides a detailed discussion, with case studies on Alexa and Sophia the robot, and the article is concluded with future directions in Section 10.

4. Need for Transparency of the Robotic System

The decision-making process and action of standard robotic systems are pre-programmed and easily verifiable, but new autonomous robotic systems, which can learn from their interactions, would be able to change their behaviour as time progresses. However, if there is no visibility about why the robot behaves or acts this way or that way, or why it makes this decision or that decision, it would be hard to trust the system. If all the activities and the inputs used by the robot to decide and act are traceable and transparent to the user, then the trust level would be high and it would be easier to control and identify any inputs responsible for ill-considered or unwanted decisions. At this point in time, there is no other technology that is more traceable and more transparent than blockchain technology (BCT). BCT has immense benefits apart from being traceable and transparent, as it provides secure communication between BC nodes, conducts a secure validation process without the need of trusted third parties, and ensures data integrity, as well as being

tamperproof, auditable, and embedding irreversibility properties, as elaborated regarding BC properties in [57]. However, BCT is resource-demanding in nature, because a set of nodes or all the nodes in the BC network must take part in the validation process, and a copy of the entirety of transactions has to be stored in each and every node. This leads to higher computation power requirements and higher energy consumption and storage demands. In general, every transaction in BC is transparent; this means that privacy is not the priority in BC and every activity is visible and traceable, as discussed extensively in a literature study in [59]. Private BC permission-based systems can be designed to limit access to the public, as discussed in [60]. However, an assistive robotic system deals with the private and personalized health and wellbeing data of users, so turning public BC to private BC is not a solution, as even within the private permission -based system, it should be designed in such a way that traceability and transparency are captured at a higher level, but personal data is concealed from any unauthorised users, and the data should not be visible to all the trusted parties of the BC network by default.

A private BC with a permission-based access mechanism could be designed, as shown in Figure 2. In this proposed BC system, the following properties would be incorporated to make it computationally efficient, and optimise energy and storage utilisation, while preserving user's privacy during the data collection or communication or storage process. It would be computationally effective if raw data is not stored in the blocks of the blockchain. A great deal of multimedia information would be collected during user and robotic interaction, and such an approach would reduce the computational overhead.

(a) The data collected from the user, ambient environment of the user, health, and raw or processed wellbeing data, etc., are all collected and securely stored within the robotic system. All data are timestamped, and an ID is assigned. Only authorised users with the correct credentials can access the data and the level of access would depend upon the access priority and access rights provided by the user, or as required by the care provider or the maintenance team or supervisor.

(b) A private BC system could be built among the robot, user's PC/PCs, and cloud storage. However, the BC would not store any raw data or encrypted data; rather it would store only the 'Merkle tree', a hash of the transaction, timestamp, and unique ID of each transaction. This way, there would be no concerns about the data leakage or visibility in the BC network. It will, thus, preserve the user's privacy in the BC system; even if hackers get into the BC system of the cloud or the PC of the user, no data would be visible. However, the stored encrypted data in the robot would be synced with the BC system that runs in the robot, the user's PC, and the cloud, so that every activity of the robot is transparently captured in the BC system.

(c) In order to maintain consistency and preserve the integrity of the BC system, a proof of stake (PoS) consensus algorithm approach could be adopted rather than the proof of work (PoW). This is because PoS blocks are assigned to validating nodes rather than miners, solving the hash math problems to validate and update the block, as described in [61]. Such an approach is more appropriate for the proposed BC framework, due to the participation of the limited but known nodes.

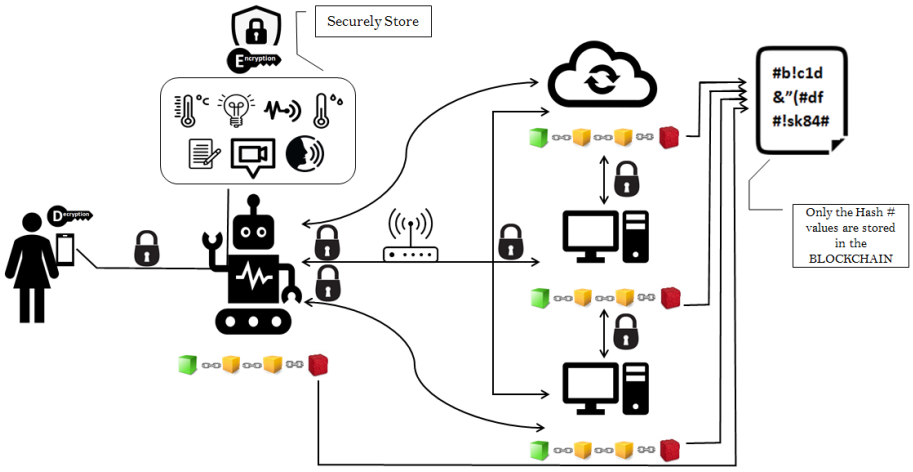

Figure 2. Proposed Resource Aware Private Blockchain Network.

5. Security and Privacy Threat Modelling

Security and privacy threat modelling depend on the situation and scenario where the assistive robot is deployed, how it is accessed or connected (if an IoT smart environment is integrated with the robot), and the number of users accessing the service from the same robot, etc. Here, three threat categories are created to mimic the real assistive robotic deployments in different scenarios and environments within the care provider context, namely: threat modelling of single user single AMRSys, threat modelling of single user single AMRSys with IoT, and threat modelling of multiuser single AMRSys with IoT.

5.1. Threat Modelling of Single User Single AMRSys

In a multimodal robotic system, communication is done via multiple channels and multiple platforms. Therefore, within the robotic sensing space, information can be leaked easily unless the right channel or the right platform is adopted during an interaction with the user, depending on the situation and the scenarios, e.g., presence of children, strangers, or intruders, etc. The robotic system must learn and know when and how to react, depending on who is present within its sensing space. Otherwise, information can easily be leaked to unintended users, inappropriate users, or an intruder, as shown in Figure 3. When the robotic system is allowed to monitor and connect remotely, more security measures should be put in place, so that a man-in-middle cannot hijack the channel, DoS and DDoS attacks do not prevail, and the remote client application interacts only if the robot approves the authenticity of the users. If an appropriate continuous authentication mechanism is not adopted for the remote users, then unauthorised users can gain easy access, e.g., if one-time authentication is used, then once the user is authenticated then anyone can access what the authenticated user can access in the presence or absence of the authenticated remote user. Therefore, an innovative continuous authentication client application must be designed to avoid data leakage to any third-party during local or remote interaction with the robot. It has been reported by IBM that, over the years, compromised credentials caused the most data breaches [66], so a more secure method of authentication and authorisation needs to be designed during local or remote connection to the robot. In order to maintain better coordination and discipline, both the user and the robot may have to support each other and signal each other during the communication, to preserve the user's privacy and protect their data. In addition, a secure channel should be used in the presence of any third-party individuals, unless the user approves it, e.g., not communicating using verbal communication in the presence of any other individuals if related to private information (maybe use a text form of communication in the presence of inappropriate or unintended persons, or a potential intruder). Therefore, it is important to detect the presence of others, recognize the individuals, assess the situation, and then

take the appropriate and necessary action, otherwise user's privacy could be easily compromised.

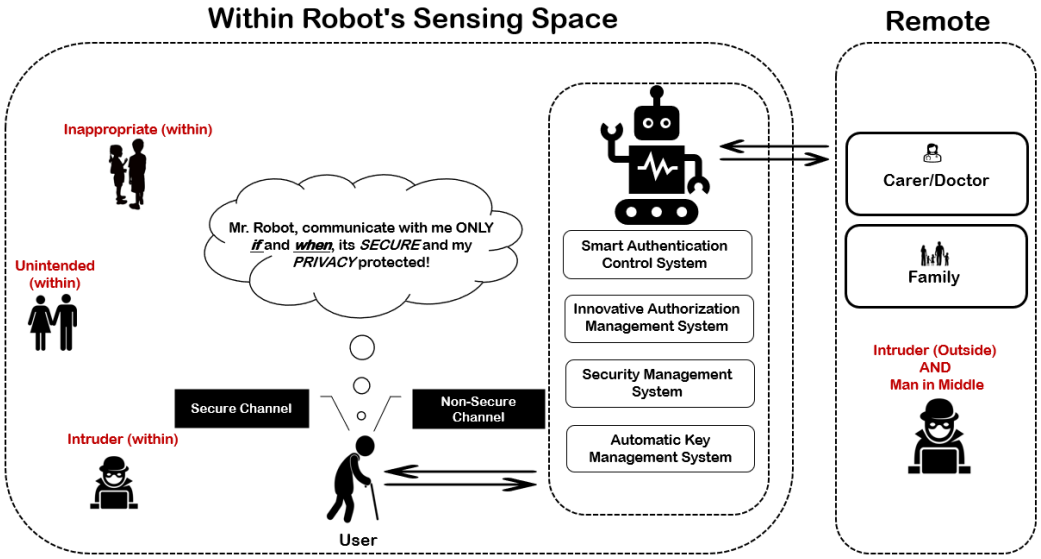

Figure 3. Threat Modelling of Single User AMRSys.

5.2. Threat Modelling of Single User Single AMRSys with IoT

If the robotic system aims to support and provide independent living to the older person in a true sense, then it needs to learn about every activity and the behaviour of the person under its roof. To provide the best ambient living environment, the robot can regulate, control, and manage the environment through the IoT systems connected to the thermostat, ventilation, lighting, window screening, heating, etc. It can monitor the health condition of the user through smart healthcare devices. It can also control and monitor the user activity and manage medication e.g., reminding what medicine to take when, as shown in Figure 4. The threat increases during the integration of the IoT in the assistive robotic system. In this IoT and robotic framework, during the interaction and integration of the IoT devices, the system should make sure that the channel is secure, keys updated, and that the IoT devices are authenticated. Moreover, no default configuration and default password should be used forever, a malicious device should be detected and replaced, and so on, as these are some of the key security concerns in IoT systems. The IoT devices and their data should be reliable, dependable, and trustable. Otherwise, an incorrect decision could be taken, inappropriate action could be made, and moreover, wrong information could be collected about the user, their health, their environment, and so on. In addition, unless security measures are in place, IoT data collected about the user and their habitat by the robot could be easily leaked to any third party and the user's privacy compromised. Integrating IoT would optimise the decision-making process, but it should not overload the computational power of the robotic system. Therefore, a fog computing approach should be integrated to filter, aggregate, control, and verify the IoT data before feeding it into the robotic system, so that only meaningful information is fed to the robotic system.

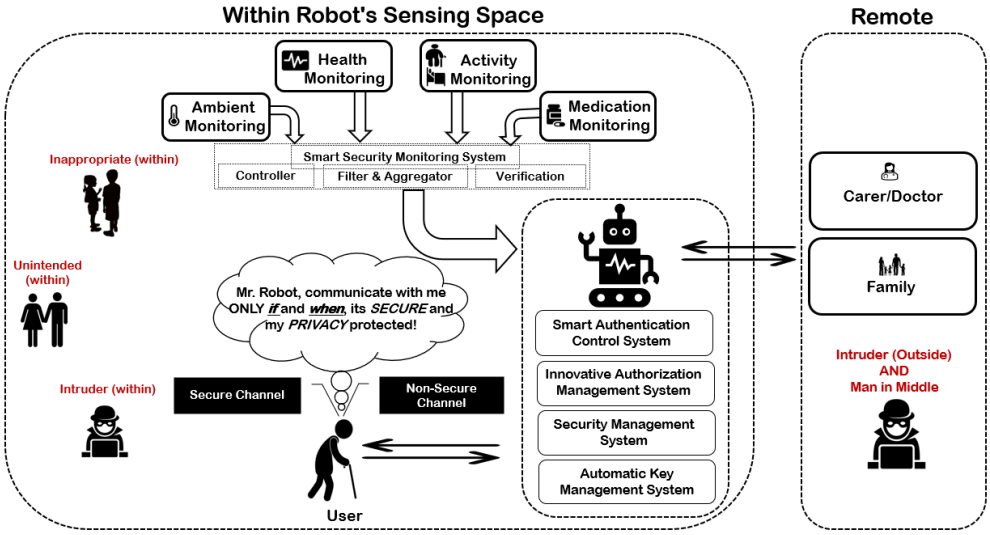

Figure 4. Threat Modelling of Single User Single AMRSys with IoT.

The security concerns in IoT are numerous and varied, there are many security challenges, and among them, the key challenges include securing resource constrained devices, authenticating and authorising battery-powered devices, and managing bugs and updates. In addition, securing the communication channel, secure integration with other systems, detecting and preventing incidents and vulnerabilities, predicting and pre-empting security issues, and ensuring data privacy and data integrity are vital [67]. Since the IoT system would be dealing with personal preference data, personal activity data, and the user's wellbeing data, it is sensitive in nature. Integrating the vulnerable IoT system with the assistive robotic system should not compromise users' data security and the user's data privacy. Moreover, the robotic system should be responsible for secure storage, key management, authentication, authorisation, and overall information management to preserve users' privacy and to protect itself from cyber-attacks, to safeguard its functionality, its OS, the attached data-generating sensors, storage, and its communication with the user.

5.3. Threat Modelling of Multiuser Single AMRSys with IoT

In a care home or care setting, to optimise the service utilisation and minimize the cost of robotic operation, a single assistive robot can be deployed to manage and provide services to multiple users. In this scenario, as shown in Figure 5, a smart and personalized wellbeing-monitoring IoT system could be integrated, coordinated, and managed by the robot for every user's living space, e.g., bedroom, shared living room, etc. However, the key challenges in this multi-user service system are the vulnerability and high chance of leakage of personal information. Secure privacy-aware communication, maintaining the secure storage of each user's information, without errors of mixing or crossing with other user's information; seamless continuous identification, authentication, and authorisation of each user; dynamic key management; and pre-emptive measures, etc. are important. In this situation, apart from leaking information to three types of people, i.e., to inappropriate children, unintended visitors, and intruders (inside or remote), now the inmates or care mates living together are potential candidates through which user's privacy could be compromised. Moreover, the robot needs to have a priority-based scheduling service with pre-emptive mechanisms, so that it maintains fairness while attending users, based on emergency and urgency. It should be designed in such a way that it does not have conflicts or become mixed up with the services it aims to provide regarding the user's needs and requests to preserve users' privacy and to protect important user data from leaking, collecting, or storing in an unintended location or with unintended users.

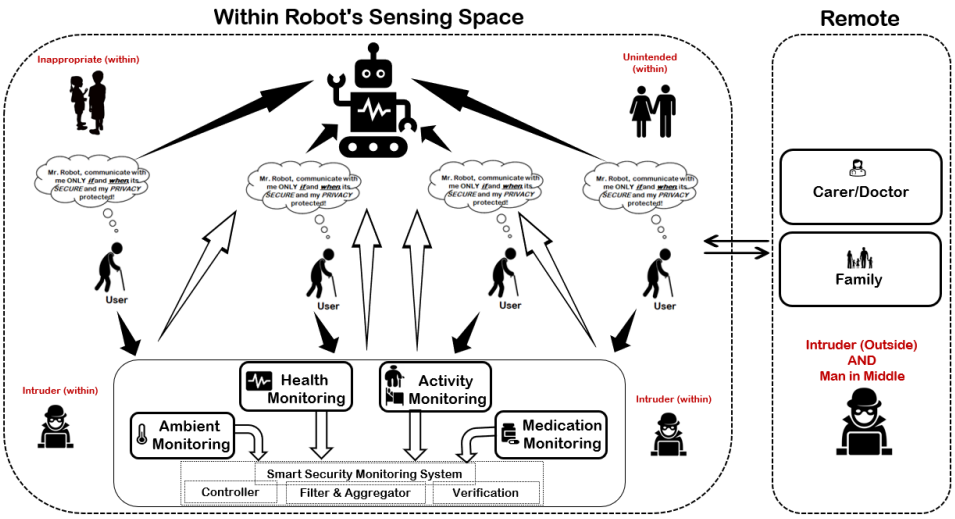

Figure 5. Threat Modelling of Multiuser Single AMRSys with IoT.

6. Security Parameters for Safeguarding and Protecting User's Data in AMRSys

In an assistive robotic system, it is the robot that controls and manages the services. The key security measures that the robot needs to maintain are highlighted in Figure 6. It is crucial to make the robotic system and its interaction with the user secure in every way, to protect and safeguard the user–robotic cyberspace and induce reliability, trust, and adoption. There are a wide range of possible attacks, so it is important to address all these fronts to protect user's data and user's privacy, as well as to preserve the service integrity of the robot, the functionality of the robot and its sensory extensions, the applications, access authorisation activity, and so on. It is important to guarantee data confidentiality, whether during interactions or storage. Data integrity and data availability are vital, but the system should also have the right access control mechanism, safe and secure remote connection, seamless software, and application upgrade process. The system should also be able to detect and invoke preventive measures pertaining to any form of intrusion, and it is important to understand the social and moral norms and basic regulations, so that user's privacy can be v preserved, irrespective of the presence of any other individuals.

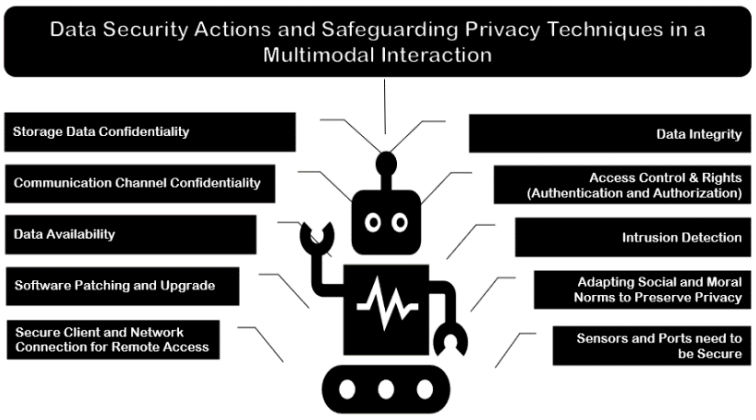

Figure 6. Security Measures for Safeguarding and Protecting User's Data and Privacy.

7. Security and Privacy Challenges and Limitations in AMRSys

There are multiple ways and means through which the robotic system's security and privacy could be compromised, and there are factors limiting the robotic system from integrating security features. Some of the domains that need attention to safeguard the interaction between the robotic system and the user are the channel or media of communication security, data integrity, data availability, unintended users, inappropriate users,

intruder, access control mechanisms and techniques, authorisation, network security, and proxy system and storage security. Other challenges for safe and seamless adoption of security features are scalability, system or device constraints, and user constraints, among others. There are also other factors that could make a robotic system vulnerable, e.g., impersonation, man-in-middle attacks, software, OS bugs, etc. The key issues and challenges, along with possible solutions are discussed below:

7.1. Data Confidentiality of a Channel between the User and Robot

This interaction could be done in multiple ways. Depending on the nature of the connection, the channel could be considered or made secure or not secure.

7.1.1. First, Via a Mobile App or Tablet App

In this method, technology such as Bluetooth or an unlicensed free frequency connection via a local home wireless router could be adopted. To facilitate a remote connection, access could also be made available via an internet connection.

7.1.2. Second, Using a GUI Attached to the Robot

In this method, a touchscreen base communication channel is used.

7.1.3. Last, One-to-One Open Communication

In this method, the user and the robot communicate directly via voice, gestures, signs, etc., without using any form of additional communication technology. This method of communication is natural, seamless, and easy to adopt.

The means of communicating in the first two methods (which uses technology) can be secured easily by adopting any current state-of-the-art encryption security mechanisms to maintain data confidentiality. However, one-to-one open communication does not adopt any technology as a medium to interact between the user and the robot. It is impossible to secure the channel if direct voice communication is used during the interaction, because it could be heard by anyone within audible range. Signs and gestures could also be easily intercepted and decrypted by anyone within the user and robot's sensing area. Thereby, information could easily be leaked to both unintended and inappropriate audiences, notwithstanding any intruders. Coded signs, signals, and words could also be used to maintain some form of confidentiality during the interaction in the presence of any third-party individual. However, this may even lead to the making of unintended decisions by the robot due to ambiguity. In addition, such codes and signs would neither be as secure as expected nor convenient for the users, especially if the users have mental health issues or some form of serious disability. Therefore, the robot needs to know when and how it should communicate with the user, to create a safe environment to protect the user's data and safeguard their privacy.

In an open communication between the user and the robot, information could easily be leaked to three categories of unauthorised user within the sensing range namely: unintended, inappropriate, and intruder. If the user approves the presence of any individual (family, friends, doctors, or nurses), privacy concerns would not arise or apply in such a scenario. In a remote access platform, any form of unauthorised access could be an attempt to steal, tamper with, or alter information, so unintended or inappropriate scenarios may not arise.

7.2. Data Integrity and Availability

It is vital to maintain data integrity and data availability, while ensuring data safety and security. Otherwise, it would become challenging to detect or be aware of any data tampering and any form of data alteration taking place during data transmission or data storage. Moreover, the stored data should be easily accessible, in a timely and reliable

manner, when and where it is needed. Who can access, their level of access, and the visibility of control over data is a different security concern altogether, which should be managed and monitored by the access control mechanisms and techniques.

7.3. Unintended Data Disclosure Issue

Within the robot or user sensing space, the presence of any adults who are not supposed to be listening to the conversation between the robot and the user would be considered an unintended listener. People could walk in, people could already be present within the sensing space (which went undetected), and if it is a public area, any adults in the public space within the sensing area are also considered unintended unauthorised individuals. Either the robot or the user, or both, should be able to recognize information leaking scenarios and situations. If public space is considered, then the forms of information leakage may not only be due to the presence of unintended adults, but could also be the presence of technological recording systems such as CCTV, which record both audio and video.

7.4. Inappropriate Data Disclosure Issue

If the unintended individuals are minors, then the individuals would be considered as inappropriate unauthorised individuals. This is critical, otherwise ethical concerns may arise, and may even lead to a negative psychological impact on the child, because of age-inappropriate conversations, interactions, and content. What to discuss, what to display, and what services to provide should be carefully considered by the robot to avoid the embarrassment, humiliation, discomfort, or awkwardness of the user and minors.

7.5. Intruders

Any device or system or individual adult or minor who aims to steal, tamper with, or destroy information can considered an intruder. It would be hard to identify and distinguish between an intruder and any unintended access attempt from authorised users, in terms of their activity. Even if activity is monitored to detect and prevent intrusion, it can be challenging to identify an attack in time, depending on the nature of the attack. An attack on a system can take multiple forms, and methods include flooding attacks, redirection attacks, replay attacks, malware attacks, etc. As such, the best first line of defence should include malware detection, patching of software flaws, white-listing, and application execution control, as well as the monitoring of activity and incorporating a network defence system if remote access is required. Above all, the designing of efficient continuous authentication and authorisation mechanisms for a successful secure access control technique is required [62].

7.6. Access Control

In order to adopt a successful access control system, the following three aspects need to be addressed:

7.6.1. Identification

Methods need to be provided so that the robot can identify the user. The user needs to be identified, so an authentication process should be in place. The data used to identify the user are critical, because their complexity to be recreated is directly proportional to the strength of the authentication mechanism that is in place to safeguard against any form of unauthorised users.

7.6.2. Authentication

In order to achieve the goal of identification, a technique and a process need to be adopted by the robot to detect and validate the authenticity and the identity of the user. The different techniques available to authenticate a user are compared in Table 3, and,

thus, Table 3 elaborates and considers the viability and feasibility of studies of the adoption of authentication mechanisms among potential AMRSys users; while, different types of authentication mechanism are also described below [63,64]:

- Password -Based Authentication: This form of authentication is one of the most common and most popular forms of authentication. However, this technique invites multiple forms of attack e.g., phishing attacks, man-in-middle attacks, brute force attacks, dictionary attacks, credential stuffing attacks, keylogger attacks, etc.
- Multi-Factor Based Authentication: This technique is more secure than password-based authentication. This is because in this approach multiple independent methods or combinations of different platforms and techniques are used; e.g., a combination of password and authentication session keys, generated using an authenticator application or through a SMS mobile phone.
- Certificate -Based Authentication: This authentication technique uses digital certificates with keys (public and private) to authenticate the user or the system that has this certificate. These certificates are presented as a proof of authenticity of the user to the server, and the server confirms the genuineness of the certificate and the certificate-issuing authority through the association of the keys with its certificate.
- Token -Based Authentication: This technique allows users to enter their credentials to the server, and the server provides a unique encrypted random string (token) that the system recognizes. In the future, without using the credentials, this token generated with the credential of the user by the server is used for authenticating. However, whoever has this token can compromise the system. This method is safer than directly using a password; however, this method is also prone to different kinds of password-based attacks, as highlighted earlier under password-based authentication.
- Biometric Based Authentication: This form of authentication uses the biometric data of an individual to uniquely identify the user. This form of authentication has gained popularity because the biometric data is associated and stays with the individual and generally does not change (facial, fingerprint, voice, retina, gait, heart signal). Moreover, it does not involve memory recall or require technical skills from the user, so it can be used by any user to identify the individual to the system. However, one of its biggest drawbacks is that it can also be easily extracted, unlike a password, token, or certificate that can be memorized or stored (locally or remotely). Moreover, biometric data, such as fingerprint, voice, and facial data, can be extracted and replicated easily in this machine learning- and AI-powered 21st century.

Table 3. Authentication Mechanisms and Adoption Analysis.

Type		Ease of Adoption			Ease of Implementation	Cost and Advantage (Adv) Disadvantage (Disadv)	Security Level
		Normal Individual (It Is Easy to Adopt)	With Health Issues				
			Have Physical Condition (It Is Easy to Adopt)	Have Mental Condition (It Is Easy to Adopt)			
Password		YES	YES, if user can remember and enter otherwise, NO	NO	YES, but challenging for serious physical and mental health issues.	LOW Adv: Change it anytime Disadv: Need to remember	LOW, if easy common and short passwords are used and if not changed for long time.
Multi-Factor		YES	YES, if user have input source, otherwise NO	NO	YES, if the right system and devices are available for the multi-factor, but challenging for physically and mentally challenged people.	LOW Adv: Use of different medium. Disadv: Need to remember some factor.	HIGH, if the second factor uses authentication app or email. SMS is not secure.
Certificate		YES	YES	YES	YES, since it is digitally stored.	LOW Adv: Can be updated any time. Disadv: User doesn't remember or possesses it, only in the system.	HIGH, but authenticating user may be challenging
Token		YES	YES, if user has hands, mouth to input, otherwise NO	NO	YES, but impossible or challenging to use for physically and mentally challenged people.	LOW Adv: New token can be created. Disadv: User must remember.	LOW, it involves possessing or remembering the token.
Biometric	Facial	YES	YES	YES	NO, a facial recognition app is required and a camera is necessary.	EXPENSIVE Adv: No need to remember. Disadv: Cannot change.	HIGH, if physically present and 3D live aspect is taken into account, otherwise it is not.
	Fingerprint	YES	YES, if the user has fingers, otherwise NO	YES, if the user has fingers, otherwise NO	NO, biometric finger print reader and app is required.	EXPENSIVE Adv: No need to remember. Disadv: Cannot change and left everywhere we touch.	HIGH, if the user is present physically and if used with second factor authentication, otherwise NO.

	Voice	YES	YES, if the user is not mute and/or deaf.	NO, if the user is mute and or deaf.	NO, voice recorder and recognition app is required.	EXPENSIVE Adv: No need to remember unless a passcode is used. Disadv: Can be regenerated by someone.	HIGH, if the user is physically present, and a second factor is considered, otherwise AI can easily spoof the voice.
	Retina	YES	YES, if the user has eyes and is not blind, otherwise NO	YES, if the user has eyes and is not blind, otherwise NO	NO, scanner and recognition app is required.	EXPENSIVE Adv: No need to remember Disadv: Can be replicated and captured from external source.	HIGH, if the user is physically present and second factor authentication is taken into account, otherwise NO.
	Gait	YES	NO	NO	NO, recording and recognition app is required.	EXPENSIVE Adv: No need to remember. Disadv: Can be replicated or captured from external.	HIGH, if accompanied with second factor authentication.
	Heart-Signal	YES	YES	YES	NO, recording and recognition app is required.	EXPENSIVE Adv: No need to remember and not visible externally. Disadv: If signal is captured, it can be re-used.	HIGH, since it cannot be captured without physical contact or within close vicinity.

7.6.3. Authorisation

When it comes to access control, apart from the identification and authentication mechanism, authorisation is important. In order to have the best control of who can connect with the robot, who can access what information, and at what level, it is best for the user to be an admin, in order to control the authorisation of the database. In addition, the access rights and access levels are stored and managed within the robot via the user, to access services from the robot. The steps to obtain services through authorisation, identification, authentication, and access rights are elaborated in Figure 7.

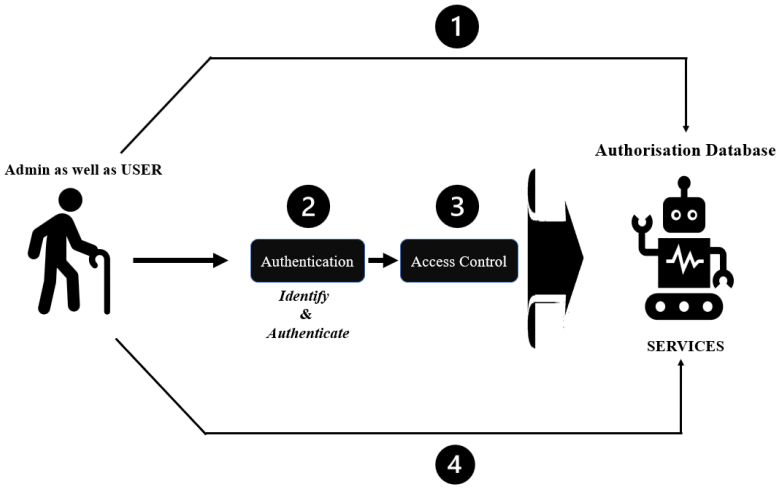

Figure 7. User as Admin for Authorisation.

7.7. Network Security and Proxy System

When remote access to the robot is invoked; any standard data IPSec security mechanism can be adopted. However, remotely connecting directly to the robot is not safe, because any cyber-attacks could lead to dysfunction or malfunction of the robot itself. Therefore, for any form of remote access, a proxy system should be incorporated to act as a firewall and safeguard the robotic system. To offload the computation power of the robot, network intrusion detection and network prevention mechanisms should be incorporated within the proxy firewall system. Having said that, a system intrusion detection and prevention system should also monitor any abnormal activities within the robotic system, to protect it from any local attacks and attacks that could not be detected by the proxy firewall.

7.8. Storage Security

The data of a user, or each of multiple users, should be securely stored; it should not be visible to anyone unless this is authorised by the user. The user's privacy should be protected and mechanisms to attain this privacy should be embedded within the system's design. To make it 2.0 secure, no raw data should be stored in a plain text version, rather it should be stored encrypted, and depending on the access rights and the level of the access rights, unique dynamic decoding keys should be provided. Moreover, as discussed earlier, to make it transparent, a lightweight BC system could be designed, in which the blocks are not the raw data or the encrypted raw data, rather only the hash and related information, along with timestamped and index-able information that are stored to enable access from secure storage, if needed.

7.9. Scalability and System Constraints

Device limitations, in terms of resources (computation power, battery power, storage, connectivity, and bandwidth), restrict the integration of resource-hungry security mechanisms. When security features are incorporated, the next challenge is the scalability issue, because this relates directly to performance, both in terms of device computation ability and network tolerance. The sensors dealing with multimedia information are resource-demanding, and adding security features strains resources further. The amount of IoT data that a robot can handle and manage, to meet real-time response requirements with a high accuracy rate, is a research domain to explore. Considering the number of sensors that would be used, Bluetooth technology might not be the best way forward compared to Wi-Fi technology, because this allows a higher number of client connections. Incorporating blockchain technology to maintain transparency and traceability will again be resource-draining, because of its demands on computation, energy, storage, and bandwidth. That is the reason why it has been proposed that the raw data should not be stored within the BC system, but only the hash and related key indexing, with identifying values stored in the blockchain blocks and not the data. In fact, it would be impossible to manage and maintain, in terms of resources, especially the storage requirement, if a copy of all data was also distributed across the nodes of the blockchain network. Thus, measures should be taken so that scalability is not an issue when IoT and Blockchain technology are integrated with a robot, and such a secure framework is proposed in Figure 2.

7.10. User Constraint

In the end, it is the user who is going to navigate, interact, and engage with the assistive robot, so the security features should not become a hurdle to adoption, because security mechanisms and techniques can complicate the way the user and the robot interact. This may involve remembering, configuring, and setting the system at the very least. The security features should be seamlessly integrated into the design and hide complexity from the users' perspective, because users are diverse in terms of their ability, skills, and physical or mental condition. It should be designed to be as user friendly as possible and easy to adopt and operate.

8. Cyber Attack Assessment on AMRSys

Table 4 elaborates the forms of attack and their possible impact on a robotic system. Depending on the attacks, the functionality, operation, and services could be affected. In the event of an attack, the impact could lead to a total shutdown of the system or to partial functioning of the system. The attacks could even lead to control of the robotic system, depending on the nature of the attacks.

Table 4. Cyber Attack Assessment on a Multimodal Robotic System.

Attack on AMRISys	Functionality of AMRISys	Control on the AMRI-Sys	Its Impact
Confidentiality - Key hijack, - Key compromise - Certificate attack, - Reconnaissance	Normal Function	No	Data would be made visible and available to a third party. The privacy of the user's data would be compromised.
Integrity - Non-repudiation, - Digital signature attack	Normal Function	No	Data alteration, tampering, and modification.

Availability - DoS, - DDoS, - Jamming, - Spamming, - Black hole, - Worm hole, - Sink hole etc.	Partly Function	Yes	It can allow the system to operate or make it inactive indirectly. However, the attacks will not completely stop the robot from functioning. It will definitively affect the services.
Access Control - Dictionary attacks, - Brute-force attack, - Man-in-middle, - Phishing, - Keylogger attack, - Password Spraying attack	Functional	Yes	The authentication process and the authorisation and control of the system could be compromised. Unauthorised users will access the services and storage would be visible unless storage is secure.
Storage - Storage account discovery, - Data Deletion, - Data Alteration or Modification	Functional	No	Data corruption, alteration, deletion; data visibility and available to a third party. Moreover, unauthorised users will see the data.
Services - Malware, - Viruses to induce a malfunction	Partly Functional	Yes	The services may stop functioning as intended.
Sensory - Replacement, - Replication - Tampering	Partly Functional	Yes	If the sensory devices are replaced or replicated, the robotic system may end up collecting or sensing incorrect or invalid data or leak the data. It may even lead to data falsification.
Network - Attack on Proxy server, - Man-in-middle attack, - Routing attack, - Media Access, - ARP attack, - Buffer overflow attack	Functional	No	It may cause dysfunction in the network and even capture traffic, but the functionality of the MRISys may be affected. The remote connection and remote delivery of information would be disrupted.

9. Discussion

In this discussion, the aspects of the transparency of the decision and service making process; privacy; security of the user's data; and security of the robot; devices connected to the robot; and its channel security are discussed.

Transparency: The proposed BC system will, not only make all the activities of the robot transparent, but will give more confidence and trust to the user, because it tracks and traces every action taken by the robot. The collected data will now be resilient to any form of data tampering and access by any unauthorised third parties. Moreover, the BC proposed in Figure 2 will not increase the utilisation of resources, rather it will optimise the resources, because the data will only be securely stored in one location, and the hash of every piece of data will be securely collected and stored in blockchain blocks. Otherwise, due to resource constraints, it would be challenging to adopt resource-hungry blockchain technology. Moreover, it would be impractical to run a blockchain within a resource-limited IoT system, as addressed by the authors of [68], so it should instead be deployed in the robot and a higher computational resource network device. This means that the proposed blockchain framework in Figure 2 will not be resource-demanding and resource hungry, particularly regarding computation power, storage, and bandwidth uti-

lisation. Moreover, the proposed BC framework will preserve the privacy of the data collected, because the actual data is not stored in the BC network, rather only one-way encrypted hash values are stored. However, all the blocks are synced with the actual data that is securely stored in the robot, and only authorised users with the right level of access rights can access the relevant information.

Privacy: It is complex in nature and a daunting task to define privacy, because it can mean different things to different people, and can vary from one individual to another. An old definition, but which is still relevant in today's context, is elaborated in a Harvard Law review, it explains that privacy is a way to protect an individual's personal space and their right not to be intruded on and to be left alone [69]. Later, the authors of [70] elaborated privacy as an aspect of one's dignity, autonomy, and ultimately the practising of freedom. Meanwhile, in this technology-driven data world, privacy is a way to control, safeguard, and protect one's information. In one way or another, privacy is all about protecting individual rights. In the universal declaration of human rights, as described in [71] by the UN (www.un.org, accessed on 12/01/22), article 12 states 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'. The revised GDPR act and related information, which is available in [72] aims to collect, use, share, and process personal data securely and with consent. Privacy in an assistive robotic multimodal system is critical, because it is linked with ethical, legal, social, and even political issues, because it deals with personal private data, and its acceptance and adoption depend on privacy. Thus, to adhere to the privacy rights declared by the UN and follow the GDPR privacy policy of the EU/UK, a robotic system needs to be designed and developed with privacy in mind. However, in this digital era, each country and each jurisdiction have their own privacy laws and regulations. The robotic system needs to comply with a varying privacy requirements, to be adopted and acceptable across boundaries, which is a daunting task.

Data and System Security: In a multimodal assistive robotic system, interaction with the users is conducted using different methods and various channels. Engagement and interaction with the users are performed through videos (visual display or recording of actions and activities, etc.), speech (audio recordings, conversations, or announcements), a tablet (on-board the robot), a remote app (phone or tablet), signs, gestures, or movement, etc. This multimodal communication could lead to leakage and exposure of information in multiple ways, to unintended and unauthorised individuals, due to the active engagement of multiple sensors and interfaces with the user all at the same time. The engagement of the user and the robot within a given space can be easily intercepted by any individual if they are close to them. Therefore, the engagement of the robot with the user would be affected by who is around the user and by events; e.g., what, when, and how to respond should be based on the nature of the data or request received from the user(s) and the presence of other individuals and the events surrounding the user.

It is vital to understand the surrounding environment of the user (any people around, who are these people, age, gender), the situation of the user (sick, medication time, hurt), the needs of the user (service based on what he/she wants), and the activity of the user (exercising, refreshing, eating), so that the multiple sensory data prompt the robotic system to respond in such a way that the user's security and privacy is preserved and well protected, both from the robotic system itself (when necessary) and other individuals (any random individuals, carers, doctor, family, etc.), depending on the need, access rights, and support requirements. The reason why user privacy should even be protected from the robot in some instances is due to the fact that, after the robotic system captures the events to be recorded, they can be accessed and viewed by certain authorised individuals to whom the user may not want to allow access, due to the nature of the activity; for example, private life: bathing, going to the toilet, and other private activities (e.g., when naked etc.) should not be recorded by the robot, unless the user's life and health and wellbeing are at risk while performing those activities. Moreover, the robot should know who is around

the user, what information can be shared where and when and, in whose presence, and to what degree. Different sensors and interfaces are incorporated and designed for a specific purpose and each sensor's activity needs to be engaged when and where it is appropriate. In addition, during interaction with the user, these sensors and interfaces of the robotic system need to be in sync and engage with the relevant and complementary IoT home and ambient sensors to optimise performance and avoid any possibility of information leakage to unintended individuals, while the vulnerabilities of lightweight limited-resource IoT sensors should be protected [73].

Moreover, to control the recorded robotic data, it should be stored securely (confidentiality, integrity, and availability should be preserved), and this can be achieved using existing state-of-the-art advanced security techniques and mechanisms. However, the processing power requirements for encryption, decryption, and preserving data integrity would be resource-demanding; therefore, the most efficient techniques need to be adopted, depending on the nature of the data (text, video, voice etc.) the robotic system processes. Moreover, key generation, key control, and key management would be challenging if third parties are avoided due to privacy concerns, so new techniques and mechanisms should be designed which are dynamic in nature, multi-factor, and involve the user in the process of safeguarding privacy. To control access to the recorded information and the interaction with the robot, a smart multi-dimensional access control mechanism should be developed, so that access to the system is not determined by a single factor of information, e.g., memorable password, pattern, or card, etc. In addition, authorisation mechanisms should be derived from the user directly or indirectly, depending on the condition and situation of the user, or trusted authorised family or friends; otherwise, the robotic system and the data could be misused. Among all these challenges, the biggest challenge in a multimodal interactive robotic system is that the communication channel is not secure during the exchange of information, and when interaction between the robot and the user is done using the voice and signs, etc. The information cannot be encrypted unless a code language is used or a secure channel is deployed via a phone, tablet, or computer, etc., otherwise, the voice- or sign-based information exchange would be easily exposed to anyone within the vicinity.

Assistive robots are generally used by older people or disabled (physically or mentally) people. As such, most of the standard authentication techniques may not be easy options to adopt, as highlighted in Table 3, in scenarios where the users are older people or disabled. This may be because of the inappropriateness of the method (e.g., use of a password for a person with dementia would not work, biometric fingerprint authentication for a fingerless person is unacceptable, etc.) or due to the lack of skills of the user. Moreover, the process of authentication should not be a one-time affair; meaning, the user should be authenticated continuously, otherwise, user information or services can be leaked easily into the hands of third-party users. If a one-time authentication technique is used to authorise services, the robot might end up providing services to other users unintentionally; e.g., in an assistive and interactive system such as Alexa, once it is woken up with the passcode, Alexa (or Siri) is not aware or does not know that it should not provide a service to user or individual except the authenticated user**.** Thus, once the Alexa system goes live, it is open for anyone to query, ask, or interact. These systems cannot differentiate between a boy or a girl, between different age groups, and do not know what is appropriate and what is not; and, therefore, they do not know what information to disclose to whom and when, and so on. In these interactive systems, once authenticated, the subsequent conversation and services provided by the robot to the user are spontaneous, which could lead to the following issues:

(a) The robot may end up providing a service without being aware of the inappropriateness of the situation and presence of other people. Therefore, this requires continuous monitoring and decision making to learn and know when the environment is safe to provide a service.

(b) Since it is authenticated once, and there is no mechanism to check the authenticity of the user continuously, other users may end up requesting a service.

Using one-time authentication and the use of a single authentication technique would not be an ideal solution for an assistive multimodal robotic system (AMRSys) if the system aims to preserve the user's data security and privacy. To eliminate the issues stated above, AMRSys needs continual authentication of the user, to interact seamlessly and only provide the necessary services securely to the intended user or to act securely under the supervision of the user. Otherwise, using a one-time authentication technique to access the resources and services of the robot will eventually make the robotic system vulnerable to data leakage, and it may even end up engaging and interacting with unintended, inappropriate, or intruding users.

In order to identify and create a safe environment, it is critical to design a smart and secure framework that would help the robot detect, identify, and make appropriate decisions and take necessary action to safeguard the user's privacy and protect the user's data if unintended or inappropriate persons, or an intruder, are present within the audible and visible sensing space. In addition to the sensory system embedded in the robot, integrating smart home and smart healthcare monitoring system environmental data with the robot would enable the robot to make well-informed and better decisions.

9.1. CASE STUDY: Security Vulnerability of Alexa (Especial Focus on Authentication)

In this vulnerability study an Alexa system as shown in Figure 8 is considered. As reported in [74], the Alexa security bug allows hackers to access the recorded voice history of a user. It has also recently been reported that there is a potential risk of user information and contact list information exposure, if any third-party skills from the Alexa skills market platform are installed, as revealed in [75]. In another incident, as reported by an independent news report, as described in [76], a user found Alexa's recordings of her voice and all her phone sync information, including the location information of the device, through Amazon. This shows that the syncing of Alexa with a phone and the cloud could potentially allow Amazon to collect personal information, and unless the user knows how to fine-tune their security settings, the possibility of leaking private information increases. In the following section, the security weakness of an Alexa system is discussed, to understand its loopholes and reveal the vulnerabilities in an interactive multimodal robotic system:

Alexa: The system does not record or go live until a wake word is used. Therefore, it seems to be protected, and in fact, the wake word is further processed at the cloud server to verify the wake-up call. It also has an inbuilt mechanism to show when it is recording, because a light indicator or audible tone will sound. Moreover, the mic or camera can also be disconnected, then it will stop listening and recording the query. Thus, many features are added to protect users' privacy and maintain data security. However, the following issues and challenges are not addressed by this advanced echo system [77].

- The system may wake up if the wake-up word is used during a conversation, without having the intention to wake up Alexa.
- If the sound of a word is similar to the wake-up word, it may still detect it as a wake-up signal.
- The system may not be recording, but it is listening; otherwise, how would the system detect a wake-up word or phrase? There is a provision to manage and control the voice recording; however, how many times and how often, would someone check if a recording was made accidentally or on purpose. Unless this is checked and managed regularly, sensitive information and data might be recorded by the system.
- Once the system is live, the system has no idea of who can access or query. It does not monitor what is appropriate to age, situations, and scenarios. It will provide the service to anyone.

- Anyone can wake up the system, simply by knowing the authenticating word, it means that anyone who can speak, can activate the system. Since the sound of a word is used to activate the process, the authentication mechanism is very insecure, mainly because it is easy and anyone within an audible vicinity can hear the code. If a voice recognition system is included, to detect and authorise the users, then knowing the sound of the passcode will not activate the service, unless the user is authorised and validated through a voice recognition authentication process.
- The system has a mechanism to recall and reread the past recoded data from the system, so anyone can listen to past recorded queries if they know the wake-up word. This is very inappropriate, as it easily leaks private and sensitive information. Medical records and problems, legal issues, and private choices including financial status and records could be leaked.

Thus, the existing privacy mechanism in place is neither effective nor efficient in managing and controlling user data and the way the user interacts with Alexa.

Figure 8. Alexa (https://www.amazon.co.uk/).

9.2. CASE STUDY: Potential Security Solution for Authentication—Sophia the Robot

In this case study Sophia the robot as highlighted in Figure 9 is considered. Apart from the amazing speech recognition ability of Sophia and human-like ability to conduct a conversation, it can also recognize individuals and see using computer vision algorithms and techniques. It can use face detection and recognition techniques to conduct a continuous authentication process [78]. This system can detect unique users continuously; however, even such humanoid robots as Sophia have limits on how and when they can conduct continuous authentication. The general issues of multimodal interaction security and privacy issues persist; however, continuous authentication can be achieved if the user is within an audible and face-to-face viewable range. Otherwise, it may not be possible to conduct continuous authentication, if:

- Eye contact and face visibility is poor.
- The user is not speaking or responding, or cannot talk or cannot respond and turn his/her back away; it would not be able to detect the user.
- If the user is blocked by a screen or object, or if the user is in another room, then even if the distance of separation is less, it would not be possible to detect and conduct continuous authentication through face and voice recognition.

Thus, for assistive and interactive robots, it is challenging to continuously authenticate a user, learn which data is private and which is not, and know if the user's question is age-appropriate or right for the present audience, or if it comes from an intruder, or if the information sought is private to the user. Therefore, in MRISys security solutions, to preserve user privacy and to protect the data and the system, a flexible multi-factor continuous authentication method is required, so that, irrespective of the circumstances; environmental conditions; and mental, physical, and psychological state of the user, the robot can track and monitor the user, to provide seamless and continuous authentication; and also so that it knows when, how, and what to communicate to the user, depending

on the situation, the circumstances, and the environment, so that data is not leaked to any unauthorised user or third party.

Figure 9. Sophia the Robot (https://www.hansonrobotics.com/).

It would be effective to use biometric data during the user continuous identification and authentication process, because this is something that the user has that is unique. However, an appropriate biometric signal should be used, so that it is easy to collect and difficult to expose. Biometric signals such as retina and facial require the user's face to be visible and eyes to be opened, and this could be inconvenient and challenging for the user, since it involves continuous eye contact. On the other hand, biometric fingerprint data requires the continuous pressing of fingers on a biometric fingerprint reader (remote or one installed on the robot); therefore, it is also highly inconvenient for the user when continuous authentication is required. However, continuous authentication is a mandatory requirement, if the robot needs to make sure that it is always providing a service only to the authenticated user in an MRISys system. Biometric signals such as the retina, face, and fingerprint can be extracted easily, without physical contact with the user, so they are easy to clone. However, biometric data such as a heart signal are not visible, unlike the face, and do not leave impressions on whatever it touches like a fingerprint, and the signal is not easily exposed without physical contact. Heart signal can be used for continuous health authentication, as highlighted by the authors of [65], but when the heart signal of a user changes because of varying physical conditions, physical activity, circumstances, and situations, it would be hard to still authenticate, because the heart signal pattern will change. In order to adopt a heart signal as biometric data for authentication, the change in signal due to physical, mental, or psychological situation should not deter the detection rate. The benefit of using the heart signal is that this signal is the only signal that is hidden from public view, does not leave traces, does not require any effort to provide, and remains active and usable only if the user is alive. On the other hand, facial data and fingerprints can be extracted or will work even after the person is dead. In addition to the heart signal, to improve accuracy and reliability for the continuous authentication process, it needs to be coupled with factors such as phone availability within the robot's proximity, tokens, or digital certificates, to ensure that it is extracted by the user's approved devices, such as a smart wristband, to avoid any form of replay attacks. As such, in this case, the user need not remember anything, or scan or touch or hold any card, to conduct the continuous authentication process. Improved detection mechanisms such as a local binary pattern in combination with other techniques, such as contrast adjustment, bilateral filter, histogram equalization, and image blending, can be adopted to improve accuracy [79].

10. Conclusions and Future Direction

Trust is one of the key factors in technology adoption, especially in health-related applications. To enhance trust, it is mandatory to safeguard users' privacy and protect

users' data from any form of cyber-attack and leaking of information to unauthorised users. In an assistive multimodal robotic system, it is a daunting task to ensure user privacy and protect user data, because there are multiple alternative channels of interaction (e.g., audio, video, gestures) that can be exploited to access personal information. Often, to improve the decision-making process and services of an assistive multimodal robot, smart home sensors and health and wellbeing monitoring systems are integrated and open new channels of multimodal interaction that could be vulnerable. Nevertheless, these alternative channels have minimal or no security mechanisms in place. This is due to their complexity, which makes the application of standard solutions challenging, from both technical and usability points of view.

This article highlighted some of the main security and privacy challenges of a multimodal assistive robotic system, with the aim of promoting investigation and new solutions to secure multimodal interactions in assistive robotic systems. We remarked that to improve users' trust, it is important to make the activity and the decision-making process transparent to them. Blockchain, with a resource-aware framework, is envisaged as a potential solution. It was discussed that controlling the assistive robot is a way forward to safeguard users' privacy and avoid data leakage to unauthorised users. It was observed that designing continuous multifactor authentication mechanism is vital, otherwise unauthorised users could easily access services and even extract user's data from the robot. However, the right trade-off between the acceptability and usability of the system must be determined. This trade-off should be related to the type of data and personal preferences. A safe adoption mechanism for remote client connection was also discussed in this article. Moreover, this article highlighted the key cyber-security issues and challenges, and suggested prospective solutions to make assistive multimodal robotic systems adoptable with high confidence among the population. Finally, this article presented and discussed a secure-by-design approach, which could be personalized to achieve an acceptable trade-off between security prompts and usability of the system for the specific user. In future, the proposed security framework solutions will be implemented, tested, and validated with an assistive multimodal robotic system in real scenarios.

Author Contributions: Conceptualisation, J.M. and A.D.N.; methodology, J.M. and A.D.N.; investigation, J.M. and A.D.N.; writing—original draft preparation, J.M. and A.D.N.; writing—review and editing, J.M. and A.D.N.; funding acquisition, A.D.N. All authors have read and agreed to the published version of the manuscript.

Funding: The work of A.D.N. was supported by the European Union under the Horizon 2020 Grant n. 955778 (PERSEO) and by the UK EPSRC with the grant EP/W000741/1 (EMERGENCE)".

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. 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.
2. 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.
3. 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.
4. Getson, C. and Nejat, G., Socially Assistive Robots Helping Older Adults through the Pandemic and Life after COVID-19. *Robotics* **2021**, *10*, 106.
5. Pu, L.; Moyle, W.; Jones, C.; Todorovic, M. The Effectiveness of Social Robots for Older Adults: A Systematic Review and Meta-Analysis of Randomized Controlled Studies. *Gerontologist* **2019**, *59*, e37–e51. https://doi.org/10.1093/geront/gny046.
6. 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.

7. Bedaf, S.; Gelderblom, G.J.; De Witte, L. Overview and categorization of robots supporting independent living of elderly people: What activities do they support and how far have they developed. *Assist. Technol.* **2015**, *27*, 88–100.
8. 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.
9. 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.
10. 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.
11. Čaić; M; Mahr, D.; Oderkerken-Schröder, G. Value of social robots in services: Social cognition perspective *J. Serv. Mark.* **2019**, *33 (4)*, 463–478.
12. Frennert, S.; Östlund, B. Seven matters of concern of social robots and older people. *Int. J. Soc. Robot.* **2014**, *6*, 299–310.
13. Sharkey, A.; Sharkey, N. We need to talk about deception in social robotics! *Ethics Inf. Technol.* **2021**, *23*, 309–16.
14. Char, D.S.; Shah, N.H.; Magnus, D. Implementing machine learning in health care—addressing ethical challenges. *New Engl. J. Med.* **2018**, *378*, 981.
15. 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.
16. Lutz, C.; Schöttler, M.; Hoffmann, C.P. The privacy implications of social robots: Scoping review and expert interviews. *Mob. Media Commun.* **2019**, *7*, 412–434.
17. Meingast, M.; Roosta, T.; Sastry, S. August. Security and privacy issues with health care information technology. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*; IEEE: New York, NY, USA, 2006; pp. 5453–5458.
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. Lee, J.D.; See, K.A. Trust in Automation: Designing for Appropriate Reliance. *Human Factors* **2004**, *46*, 50–80. https://doi.org/10.1518/hfes.46.1.50_30392.
20. Ben-Ari, M.; Mondada, F. Robots and their applications. In *Elements of Robotics*; Springer: Cham, Switzerland, 2018; pp. 1–20.
21. Friis, D. Industrial robots–definition and classification. *World Robot.* **2016**, 25–34.
22. Hersh, M. Evaluation framework for ICT-based learning technologies for disabled people. *Comput. Educ.* **2014**, *78*, 30–47.
23. Kachouie, R.; Sedighadeli, S.; Khosla, R.; Chu, M.-T. Socially Assistive Robots in Elderly Care: A Mixed-Method Systematic Literature Review. *Int. J. Hum.-Comput. Interact.* **2014**, *30*, 369–393. https://doi.org/10.1080/10447318.2013.873278.
24. Khosla, R.; Chu, M.-T.; Khaksar, S.M.S.; Nguyen, K.; Nishida, T. Engagement and experience of older people with socially assistive robots in home care. *Assist. Technol.* **2019**, *33*, 57–71. https://doi.org/10.1080/10400435.2019.1588805.
25. Oviatt, S. (2003). User-centered Modeling and evaluation of multimodal interfaces. *Proc. IEEE*. **2003**, *91*, 1457–1468. https://doi.org/10.1109/JPROC.2003.817127.
26. Di Nuovo, A.; Broz, F.; Wang, N.; Belpaeme, T.; Cangelosi, A.; Jones, R.; Esposito, R.; Cavallo, F.; Dario, P. The multi-modal interface of Robot-Era multi-robot services tailored for the elderly. *Intell. Serv. Robot.* **2018**, *11*, 109–126.
27. Di Nuovo, A.; Varrasi, S.; Lucas, A.; Conti, D.; McNamara, J.; Soranzo, A. Assessment of Cognitive skills via Human-robot Interaction and Cloud Computing. *J. Bionic Eng.* **2019**, *16*, 526–539. https://doi.org/10.1007/s42235-019-0043-2.
28. Chen, S.; Epps, J. Multimodal Coordination Measures to Understand Users and Tasks. *ACM Trans. Comput. Interact.* **2020**, *27*, 1–26. https://doi.org/10.1145/3412365.
29. Andries, M.; Simonin, O.; Charpillet, F. Localization of Humans, Objects, and Robots Interacting on Load-Sensing Floors. *IEEE Sensors J.* **2015**, *16*, 1026–1037, https://doi.org/10.1109/JSEN.2015.2493122.
30. Li, Q.; Liu, Y.; Meng, S.; Zhang, H.; Shen, H.; Long, H. A dynamic taint tracking optimized fuzz testing method based on multimodal sensor data fusion. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 1–21, https://doi.org/10.1186/s13638-020-01734-0.
31. Qu, Y.; Zhang, G.; Zou, Z.; Liu, Z.; Mao, J. Active Multimodal Sensor System for Target Recognition and Tracking. *Sensors* **2017**, *17*, 1518. https://doi.org/10.3390/s17071518.
32. Bellotto, N.; Hu, H. A Bank of Unscented Kalman Filters for Multimodal Human Perception with Mobile Service Robots. *Int. J. Soc. Robot.* **2010**, *2*, 121–136. https://doi.org/10.1007/s12369-010-0047-x.
33. Al-Qaderi, M.K.; Rad, A.B. A Multi-Modal Person Recognition System for Social Robots. Applied Sciences. 8. 387. https://doi.org/10.3390/app8030387.
34. Krupke, D.; Steinicke, F.; Lubos, P.; Jonetzko, Y.; Gorner, M.; Zhang, J. Comparison of Multimodal Heading and Pointing Gestures for Co-Located Mixed Reality Human-Robot Interaction. **2018**, 1–9. https://doi.org/10.1109/IROS.2018.8594043.
35. Tan, Ying & Sun, Zhe & Duan, Feng & Solé-Casals, Jordi & Caiafa, Cesar. A multimodal emotion recognition method based on facial expressions and electroencephalography. Biomedical Signal Processing and Control, Volume 70, September 2021, 10302970; pp. 1–11. https://doi.org/10.1016/j.bspc.2021.103029.
36. Zhang, J.; Wang, B.; Zhang, C.; Xiao, Y.; Wang, M.Y. An EEG/EMG/EOG-based multimodal human-machine interface to real-time control of a soft robot hand. *Front. Neurorobotics* **2019**, *13*, 7. https://doi.org/10.3389/fnbot.2019.00007.
37. Gao, Q.; Liu, J.; Ju, Z. Hand gesture recognition using multimodal data fusion and multiscale parallel convolutional neural network for human–robot interaction. *Expert Syst.* 38, no. 5 (2021): e12490. . https://doi.org/10.1111/exsy.12490.

38. Pasqui, V.; Saint-Bauzel, L.; Zong, C.; Clady, X.; Decq, P.; Piette, F.; Michel-Pellegrino, V.; El Helou, A.; Carré, M.; Durand, A.; et al. Projet MIRAS: Robot d'assistance à la déambulation avec interaction multimodale. *IRBM* **2012**, *33*, 165–172. https://doi.org/10.1016/j.irbm.2012.01.017.
39. Mohammad Hossein Taheri. Multimodal Multisensor Attention Modeling. Ph.D. Thesis, NottingHam Trent University, Nottingham, UK, 2020. http://irep.ntu.ac.uk/id/eprint/41691.
40. Urquhart, L.; Reedman-Flint, D.; Leesakul, N. Responsible domestic robotics: Exploring ethical implications of robots in the home. *J. Information, Commun. Ethic-Soc.* **2019**. https://doi.org/10.1108/JICES-12-2018-0096.
41. Escalera, S.; Gonzalez, J.; Baro, X.; Shotton, J. Guest Editors' Introduction to the Special Issue on Multimodal Human Pose Recovery and Behavior Analysis. *IEEE Trans. Pattern Anal. Mach. Intell.* **2016**, *38*, 1489–1491. https://doi.org/10.1109/TPAMI.2016.2557878.
42. Umar, S.; Mosisa, E.K. A Survey on Evolution of Cognitive Robotics with Internet of Things. *Int. J. Sci. Res. Sci. Eng. Technol.* Vol 8, Issue 2, **2021**, 337–344.
43. Simoens, P.; Dragone, M.; Saffiotti, A. The Internet of Robotic Things. *Int. J. Adv. Robot. Syst.* **2018**, *15*, 172988141875942. https://doi.org/10.1177/1729881418759424.
44. Harman, H.; Chintamani, K.; Simoens, P. Robot Assistance in Dynamic Smart Environments—A Hierarchical Continual Planning in the Now Framework. *Sensors* **2019**, *19*, 4856. https://doi.org/10.3390/s19224856.
45. Kamilaris, A.; Botteghi, N. The penetration of Internet of Things in robotics: Towards a web of robotic things. *J. Ambient Intell. Smart Environ.* **2020**, *12*, 491–512. https://doi.org/10.3233/AIS-200582.
46. Cesar, C.; Lucas, A. Hacking Robots Before Skynet. *IOActive Website* **2017**, 1–17.
47. Kim, T.; Kang, B.; Rho, M.; Sezer, S.; Im, E.G. A Multimodal Deep Learning Method for Android Malware Detection Using Various Features. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 773–788. https://doi.org/10.1109/TIFS.2018.2866319.
48. 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.
49. 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.
50. 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.
51. Shakir, M.; Aijaz, A. IoT, Robotics and Blockchain: Towards the Rise of a Human Independent Ecosystem. 2018.
52. Haden, C.; Amirabdollahian, F. A Call for Stronger Privacy Protections to Promote the Development of Ethical Domestic Robots. **2021**, 31-32. https://doi.org/10.31256/Gy2Wm9H.
53. Bourimi, M.; Tesoriero, R.; Villanueva, P.G.; Karatas, F.; Schwarte, P. Privacy and Security in Multi-modal User Interface Modeling for Social Media. **2011**, 1364–1371. https://doi.org/10.1109/PASSAT/SocialCom.2011.49.
54. Wei, F.; Zeadally, S.; Vijayakumar, P.; Kumar, N.; He, D. An Intelligent Terminal Based Privacy-Preserving Multi-Modal Implicit Authentication Protocol for Internet of Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3939–3951. https://doi.org/10.1109/TITS.2020.2998775.
55. Aditya, U.S.; Singh, R.; Singh, P.K.; Kalla, A. A Survey on Blockchain in Robotics: Issues, Opportunities, Challenges and Future Directions. *J. Netw. Comput. Appl.* **2021**, *196*, 103245.
56. Henson, V.; Henderson, R. Guidelines for using compare-by-hash. 2005.
57. De Leon, D.C.; Stalick, A.Q.; Jillepalli, A.A.; Haney, M.A.; Sheldon, F.T. Blockchain: Properties and misconceptions. *Asia Pac. J. Innov. Entrep. 11*(3), pp.286-300 **2017**.
58. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **21**, pages 115–158 **2021**, .
59. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* **2019**, *8*, 100107.
60. Wüst, K.; Gervais, A. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*; IEEE: Piscataway Township, NJ, USA, 2018; pp. 45-54.
61. Leonardos, S.; Reijsbergen, D.; Piliouras, G. Presto: A systematic framework for blockchain consensus protocols. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1028–1044.
62. CESG. Information Security Arm of GCHQ, 2015. Common Cyber Attacks: Reducing the impact, .
63. Velásquez, I.; Caro, A.; Rodríguez, A. Authentication schemes and methods: A systematic literature review. *Inf. Softw. Technol.* **2018**, *94*, 30–37.
64. Amin, R.; Gaber, T.; ElTaweel, G.; Hassanien, A.E. Biometric and traditional mobile authentication techniques: Overviews and open issues. In *Bio-Inspiring Cyber Security and Cloud Services: Trends and Innovations*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 423-446.
65. Enamamu, T.; Otebolaku, A.; Marchang, J.; Dany, J. Continuous m-Health data authentication using wavelet decomposition for feature extraction. *Sensors* **2020**, *20*, 5690.
66. IBM. Available online: https://www.ibm.com/uk-en/security/data-breach (accessed on 10 October 2021).
67. IBM. Available online: https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/), reported on 2017 and updated in 2020 by Anna Gerber and Satwik Kansal (accessed on 11 October 2021).

68. Marchang, J.; Ibbotson, G.; Wheway, P. Will blockchain technology become a reality in sensor networks? In *2019 Wireless Days (WD)*; IEEE: Manchester, UK , 2019; pp. 1–4
69. Warren, S.D.; Louis, D. Brandeis. "The right to privacy". In *Harvard Law Review 4:5*; 1890; pp. 193–220.
70. Ferdinand David Schoeman. *Privacy and Social Freedom*; Cambridge University Press: Cambridge, UK, 1992.
71. UN, Article 12. Available online: www.un.org (accessed on 20 November 2021).
72. GDPR. Available on https://gdpr.eu/data-privacy/ (accessed on 21 December 2021).
73. Ingham, M.; Marchang, J.; Bhowmik, D. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET Inf. Secur.* **2020**, *14*, 368–379.
74. BBC. Available online: https://www.bbc.co.uk/news/technology-53770778, reported on 13 August 2020 (accessed on 1 December 2021).
75. Lentzsch, C.; Shah, S.J.; Andow, B.; Degeling, M.; Das, A.; Enck, W. Hey Alexa, is this Skill Safe? Taking a Closer Look at the Alexa Skill Ecosystem. In *28th Annual Network and Distributed System Security Symposium (NDSS 2021). The Internet Society*. San Diego, California and Online, 2021.
76. Independent. Available online: https://www.independent.co.uk/life-style/gadgets-and-tech/alexa-amazon-echo-voice-recordings-b1943527.html, reported 23 October 2021 (accessed on 1 December 2021).
77. Amazon. Available online: https://developer.amazon.com/en-GB/alexa (accessed on 17 November 2021).
78. Hanson Robotic, Spphia. Available online: https://www.hansonrobotics.com/sophia/ (accessed on 21 December 2021).
79. Bah, S.M.; Ming, F. An improved face recognition algorithm and its application in attendance management system. *Array* **2020**, *5*, 100014.