Access Control Architecture of Assistive Robots for Physical Activity Wellbeing Data

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

Access Control Architecture of Assistive Robots for Physical Activity Wellbeing Data

Kavyan Zoughalian
Department of Computing. Sheffield Hallam University
Advanced Wellbeing Research Centre (AWRC)
Sheffield, United Kingdom
k.zoughalian@shu.ac.uk

Jims Marchang
Department of Computing. Sheffield Hallam University
Advanced Wellbeing Research Centre (AWRC)
Sheffield, United Kingdom
jims.marchang@shu.ac.uk

Alessandro Di Nuovo
Department of Computing. Sheffield Hallam University
Advanced Wellbeing Research Centre (AWRC)
Sheffield, United Kingdom
a.dinuovo@shu.ac.uk

Abstract—Multimodal Assistive Robots (MARs) present innovative opportunities in healthcare, yet they pose significant security and privacy challenges. Our research addresses these concerns using an architecture inspired by the Authentication, Authorization, and Accounting (AAA) framework. The proposed architecture is applied to an access control system using the Robot Operating System (ROS) utilising a Fitbit tracker dataset. We introduce a fine-grained, dual approach combining policy-based and attribute-based access controls to safeguard patient data confidentiality, particularly in wellbeing contexts. This paper details our novel access control mechanism within ROS, illustrating the interaction experience between the robot and the stakeholders. The paper's findings contribute to applying a user-centric, secure access framework to a real-world use case, considering organisational policies for a multimodal assistive robot in the healthcare domain.

I. Introduction

The intersection of technology and healthcare has given rise to a promising opportunity in multi-modal assistive robotic systems (MARs). These innovative systems hold a vast possibility to revolutionise the healthcare landscape by contributing valuable contributions to various aspects of patient care, such as supporting independent living, providing personalised care, enhancing patient outcomes, and even limiting the escalating expenses associated with healthcare provision [1] [2]. As MARs continue to demonstrate their capability to enrich and streamline healthcare services, they face significant complex challenges in the domains of security and privacy. The integration of these robotic systems into healthcare environments necessitates the protection of sensitive patient information, as well as the facility for a robust mechanism to manage human-robot interactions. Regarding these considerations, access control mechanisms emerge as pivotal components, serving as protectors that ensure only authorised individuals can access and manage patient data. This paper discusses the critical role of access control mechanisms within the domain of MARs in healthcare, enlightening their importance while enabling the integration of assistive robotic systems into the healthcare ecosystem. This research aims to identify and assist with the challenges and opportunities that remain at the crossroads of technology, healthcare, security, and privacy.

The conventional one-time authorisation approach opens access to intruders and potential unauthorised users. Therefore, it is crucial to secure the channel of communication to preserve the user's right to privacy. Consequently, safeguarding the communication channel becomes imperative to uphold users' privacy rights. This concern aligns with the findings of recent research [3], which explored the acceptability of technology and the perspectives of elderly individuals regarding the monitoring of their daily living activities. Through semi-structured interviews with adults, this study revealed a positive perception of the necessity for assistive technology.

Control of a user's access authenticity and spoofing prevention mechanisms for such authentication systems result in a more reliable authentication, authorisation and accounting (AAA) architecture [4]. To ensure the access request to the resource is valid, the authentication is not enough; hence, access authorisation becomes necessary. [5] Describes the problem in the networking scenario, where the access first authenticates, then authorises using the defined access policy to control the access to the resources based on the requirements of the network and its user. The research adopts the 802.1x framework and x.509 identity certificate for a network access control approach. It uses an authorisation infrastructure based on security assertion markup language (SAML) statements, role-based access control (RBAC) model, and extensible access control markup language (XACML) as the primary language for presenting authorisation policies. Although the concept of AAA is designed for networks, the technicality of such systems may not be relevant to the problem statement of this research as the human-robot interaction comes into play; however, the concept is transferrable and adapted to a defined access control mechanism for MARs. Therefore, further investigation is

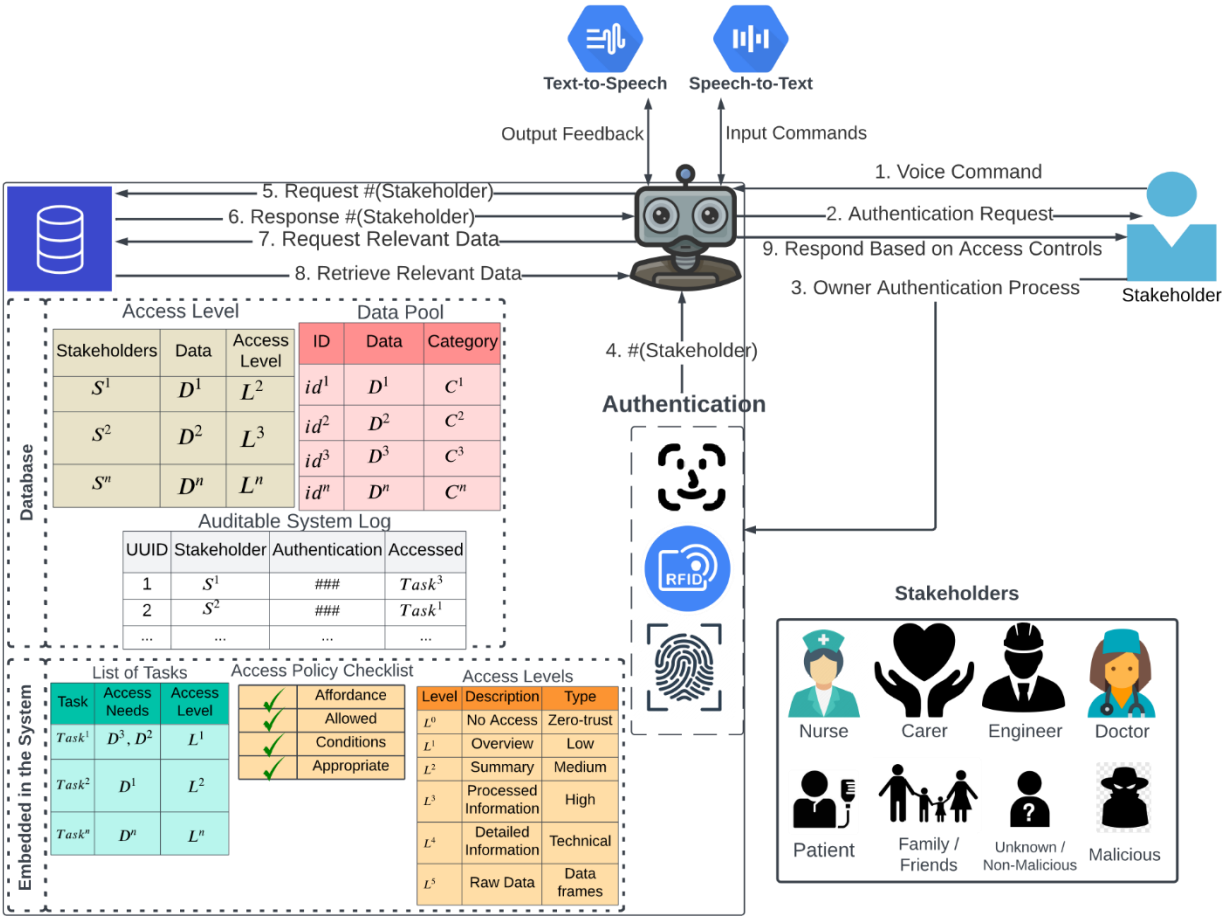

Fig. 1. Access Control Mechanism Framework, Demonstrating the Interaction Between Identified User and the Robot

required to enhance the overall system by adopting similar concepts.

Moreover, recent global events, such as the pandemic, have provided valuable insights into the effective adoption of digital solutions [6]. This review underscores the importance of technological advancements in addressing healthcare challenges.

To address privacy concerns beyond informational privacy, policy development and control definition play a pivotal role in establishing the boundaries for safeguarding patient privacy [7]. Patients may form social-emotional bonds with their assistive robots, influencing their willingness to share information, as discussed by [8]. This phenomenon introduces ethical and privacy questions, including determining the extent and timing of data access, factors affecting data access, data retention periods, and the authorisation process.

In this context, recent research on task-based access controls contributes novel insights into the architecture and enforcement layer, as well as joint modelling for assistive robots [9]. They proposed a roadmap for policy development by addressing the objectives layer and introducing activity-centric access control. Furthermore, they explored the potential integration of task planning and physical access control in humanoid assistive robots. Although the paper presents an astute view of an activity-centric task-based physical access control, information and data-focused access control can be designated as a research gap in the paper.

Moreover, Marchang et al., in their extensive review of data security and user privacy in Assistive Multimodal Robotic Systems (ARMSys) for healthcare, specified vital security and privacy necessities for ARMSys by analysing data leakage and privacy concerns in a multi-modal setting [10], the study proposes improving user trust by implementing transparent decision-making processes. The paper also discusses authentication challenges and proposes a secure-by-design approach that can be personalised based on data types and individual preferences. However, the suggested security framework solution remains theoretical, and the implementation aspects present potential areas for further research and development in ARMSys security and privacy.

II. Methodology

The proposed access control mechanism in Figure 1 illustrates a framework of the robot's access control process, presenting an overview of the human-robot interaction procedures. The

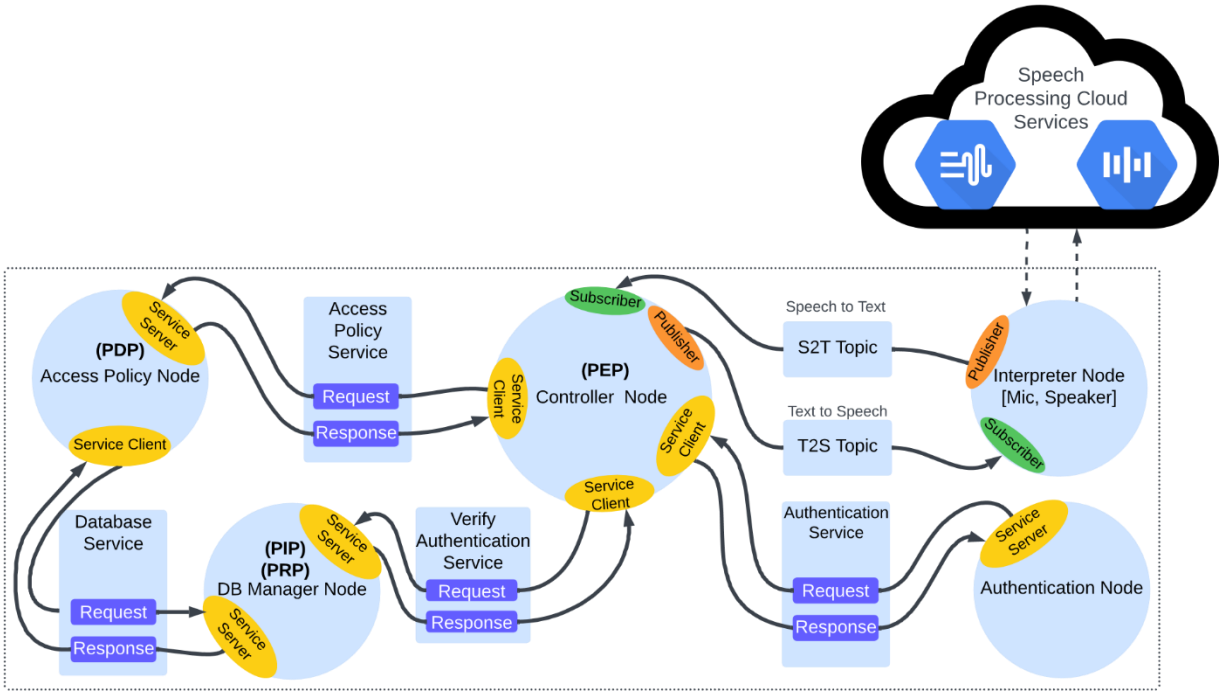

Fig. 2. ROS Level Communication and Nodes of the Overall Framework

human-robot input and output interaction via voice, using speech-to-text and text-to-speech recognition. The framework introduces a crafted access control policy designed to govern the dissemination of sensitive information in an independent living environment.

```
ros@ros:~$ ros2 node list
/access_control
/authentication_node
/controller_node
/database_node
/speech_to_text_publisher
```

Fig. 3. Showing the Nodes Running on ROS

A. Authentication, Authorisation and Accounting (AAA)

The framework highlights the AAA security framework. Authentication of the user plays a vital role in an access control mechanism as the user must be identified to specify the authorised data to access. After that, the robot refers to the role-based access rights within its database to check the authorisation level. However, simply having the right to access the requested information does not ensure the fine-grained security and privacy of the data owner; accessing the same information may not be relevant depending on the user's intentions and objectives. Hence, the robot requires more context on the nature of the request attributes and performs various checks embedded in the system as the access policy checklist. Whether the data is available, the user has permission to access the data, attributes of the access, and exceptions of those attributes. For example, a nurse requests access to view a patient's restricted heart rate data, wherein in a standard scenario, it is permitted to do so, but according to the staff rota, the request is not made within their working hours. Thus, the access must be denied. However, in the same scenario, the nurse was called in for an emergency visit because of a health-related incident; in such a scenario, the information is required for them to perform their task, and access must be granted. Consequently, the authorisation of the access depends on the context of the request. Finally, accountability clarifies the system's decision-making, which is visible on the system log stored in the robot's database.

B. Stakeholders

The proposed framework includes stakeholders within a MARs-enabled smart home in the healthcare domain. The potential users included in this scenario include nurses, carers, engineers, and doctors who may need to interact with the system to retrieve patients' wellbeing data to assess the health of the data owner. Furthermore, to expand the stakeholders, internal users such as the patient, family members, guests, internal intruders, and the external participants to include in the framework are unknown users and external intruders, which all bring their own unique complexities to the framework. However, the current stakeholders from Figure 4 were selected for a direct focus on the framework of an access control mechanism interacting with MARs.

C. Robot Operating System (ROS)

Figure 2 presents the internal process within the context of MARs. The Robotic Operating System (ROS) nodes of the access mechanism are extended between multiple nodes to avoid a single point of failure. Also, by spreading the system's functionality across various processes, fault tolerance and

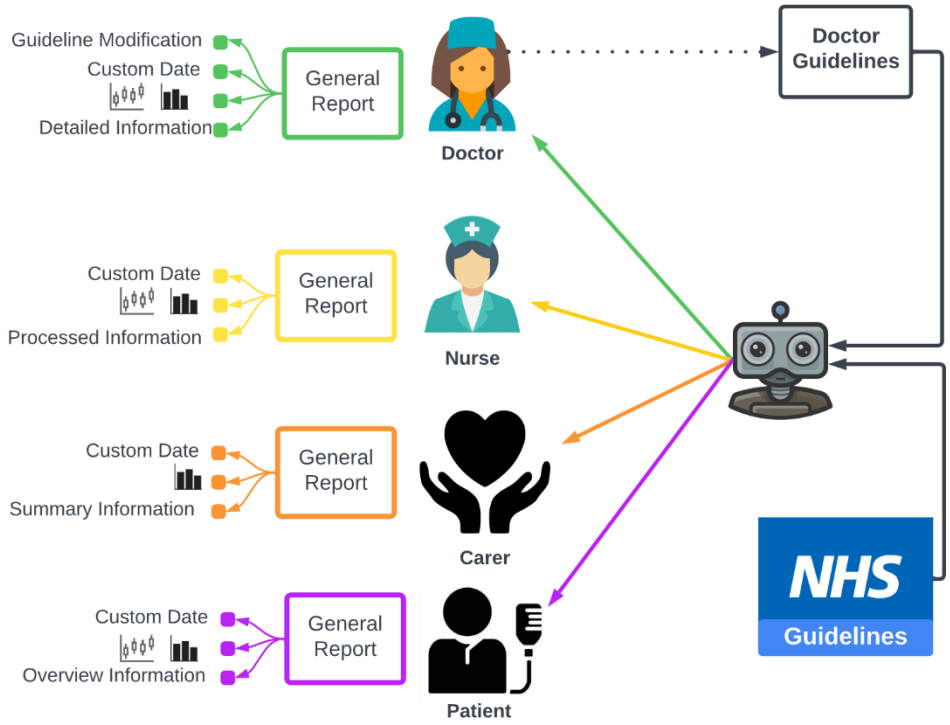

Fig. 4. Activity Information Based on NHS Guidelines and Doctor Recommendations

error handling become straightforward. In the event of a node failure, the rest of the nodes can respond by providing feedback to the user to prevent hurdles in communication. To present the evidence for this argument, the ps aux command is used to showcase the processes running on the machine's operating system in Figure 8.

The system's logic, from user input to action execution, is directed by the controller node, a pivotal component responsible for the overall process flow. User inputs are meticulously processed by the interpreter node, which forwards the information to the controller node for authentication confirmation. After that, the access policy node comes into play, conducting a meticulous checklist to determine whether the requested access should be granted or rejected. The outcome of this process is conveyed back to the user in the form of feedback, ensuring transparency and user awareness.

D. National Health Service Physical Activity Guidelines Policy

In developing a physical activity and wellbeing-related access policy, it is essential to ensure the guidelines are from reliable and evidence-based sources. The National Health Service (NHS) website serves as an authoritative reference for formulating policies to promote healthy lifestyles, particularly in the context of physical activity for adults aged 19 to 64 years [11].

The NHS provides a wealth of up-to-date information on exercise guidelines, health recommendations, and evidence-backed strategies for maintaining an active lifestyle. Accessing the NHS website lets policy developers stay informed about the latest research findings and health recommendations related to physical activity.

One key advantage of using the NHS website as a reference is the credibility and trust associated with a national healthcare service. The content on the NHS website undergoes rigorous review processes and is often based on scientific research and expert consensus. The review process ensures the access policy is grounded in accurate and reliable information.

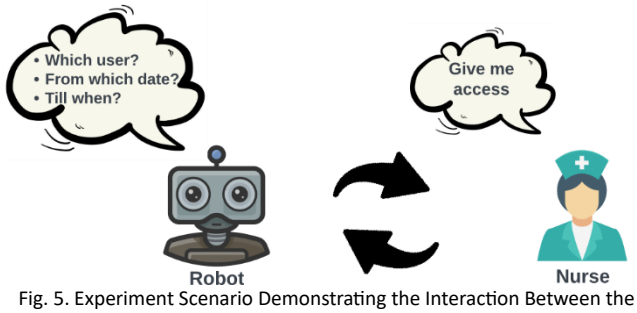

Fig. 5. Experiment Scenario Demonstrating the Interaction Between the Robot and Nurse

The guidelines emphasise the strengthening activities; this information is not directly available in the dataset [12]. We'll assume that 'VeryActiveMinutes' and 'FairlyActiveMinutes' could indicate strengthening activities. We can also consider 'FairlyActiveMinutes' as moderate intensity and 'VeryActiveMinutes' as vigorous intensity. The guidelines recommend adults exercise at least 150 minutes of moderate-intensity or 75 minutes of vigorous-intensity per week.

Additionally, it is recommended to spread the exercise over 4-5 days a week.

In this paper, we present a use case of the system using the Fitbit tracker public dataset, with the policy knowledge gathered from the NHS guidelines.

III. Experiments and Discussion

In our experiment, we simulate a scenario where a nurse interacts with an assistive robot to monitor a patient's wellbeing. The robot, equipped with access to detailed patient records, including step count, distance travelled, physical activity duration, and activity intensity, plays a crucial role. It not only provides these data but also understands health guidelines, enabling it to offer tailored recommendations on the patient's activity progress. This functionality is pivotal for the nurse, who relies on the robot's verbal feedback and visual graphs to analyse the patient's physical activity effectively. This section delves into the specific inputs and outputs of this scenario, showcasing the robot's advanced capabilities. Additionally, we provide a detailed examination of data access logs, reinforcing the transparency and verifiability of our system in a real-world healthcare setting.

The application of this system is particularly relevant within a realistic user-centric healthcare scenario where the assistive robot serves as the custodian of critical patient wellbeing data. The findings of this study illuminate the potential benefits of this approach, including the delegation of the burden of responding to wellbeing-related queries to the robot. By doing so, the study asserts that the system can effectively mitigate the human error factor. Additionally, the interaction results can be of great use to the stakeholders to provide the necessary information. thereby enhancing the overall quality of healthcare provision.

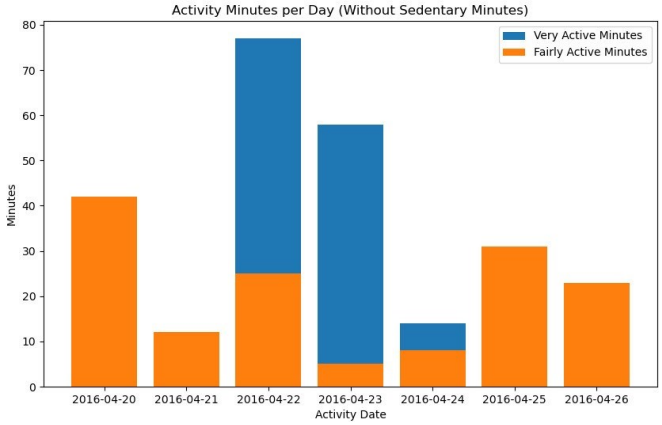

Fig. 6. Bar Chart Output of the Request to be Used by the Nurse to Identify Physical Activity Patterns and Daily Comparisons

Figure 4 showcases the practical implementation of our proposed access control policy in a real-world scenario. This is further exemplified in Figure 5, which depicts a nurse interacting with the robot. In this scenario, the nurse requests specific wellbeing data for a user by inputting the user's identifier and the desired date range. Following successful

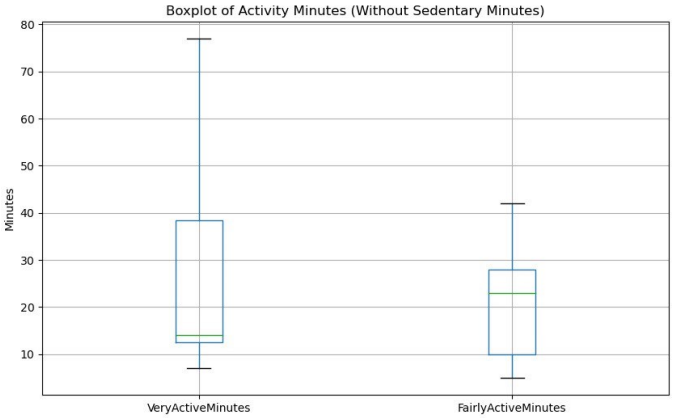

Fig. 7. Plot Box Output of the Request to Identify the Consistency of the Physical Activity

authentication, the robot prompts the nurse for three key pieces of information: the user's identifier, the start date, and the end date for the requested data. This process ensures that access to data is granted only after verifying the necessary credentials and input requirements. Consequently, the robot performs the requisite access checks and, upon validation, furnishes the nurse with the relevant wellbeing data, thereby assisting in the healthcare process efficiently and securely.

Figure 6 and Figure 7 are presented on the robot's display, along with summarised processed information based on the voice input of: "from 20th of April 2016, till 26th of April 2016 for the user 4388161847".

TABLE I Data Requested from the Dataset by the Nurse

ID	Date	Very Active	Fairly Active	Sedentary
4388161847	4/20/2016	19	42	696
4388161847	4/21/2016	7	12	853
4388161847	4/22/2016	77	25	945
4388161847	4/23/2016	58	5	749
4388161847	4/24/2016	14	8	584
4388161847	4/25/2016	11	31	1054
4388161847	4/26/2016	14	23	673

Table I presents the data that the system used to provide the information to the nurse. This information is retrieved from the dataset stored in the system.

The multi-process capabilities of the system are evidenced in Figure 8. The overall system is spread between multiple nodes, and each node runs on a separate process, meaning the system's availability is not interrupted by a single node failure. In the event of a disruption of the nodes in the system, the rest of the nodes can be programmed to notify the user of the error using the regular communication channel to maintain seamless human-robot interaction.

Figure 9 shows the access log system; to prioritise accountability and auditability, these logs meticulously record inputs and the decision-making of the outputs, thereby enhancing transparency and reinforcing accountability.

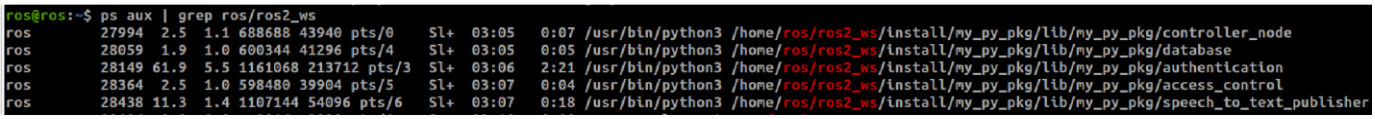

Fig. 8. Process Identifier of the System Nodes

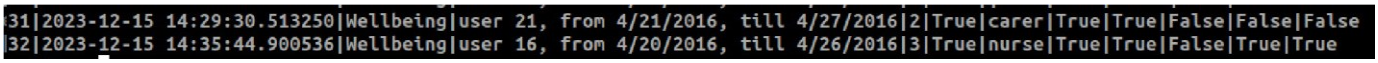

Fig. 9. Accountability of the System by Using Logs of the Information Requests and Interactions

IV. Considerations and Future Work

The access control policy must consider the prevailing conditions of the situation. It discerns whether the request is made based on exceptional conditions, providing the concept of break glass. To elaborate, a doctor may not be working at the time of the request, according to the rota, on an exceptional visit due to the patient's lack of wellbeing. The request may be granted given prior authorisation embedded as a policy. The authority to make this distinction is imperative as it influences the appropriateness of sharing the requested information. In such an emergency scenario, the policy may prioritize information sharing for critical decision-making but with a much higher accountability log registers, whereas, under normal circumstances, a more stringent evaluation might be applied. Moreover, the future work required for further details into how the robot will define context and the fine line between normal, exceptional scenarios and risks involved with a context-aware access control for MARS.

Central to its architecture is a sophisticated access control framework, meticulously designed to consider both authorized access levels and role-specific permissions. This dual-layered approach guarantees that data access is meticulously regulated, aligning with the distinct roles and privileges of involved stakeholders. The imperative for robust accountability necessitates a system that is both tamper-proof and transparent, fostering enhanced trust in human-robot interactions. Further work is required to enhance the features of the access mechanism and to bridge the gap between human-robot trust.

Looking ahead, a key focus for future development is the implementation of secure real-time data collection. This advancement will ensure the system consistently operates with the most current data, further solidifying its effectiveness and reliability in dynamic environments.

V. Conclusion

In conclusion, this study introduces a novel access control mechanism for assistive robots in healthcare, addressing crucial security and privacy challenges by looking at authentication, authorisation, and accounting. Our user-centric approach, mindful of stakeholder roles and context-specific information requests, ensures a more secure and private healthcare system. The integration of assistive robots into healthcare ecosystems is highlighted by implementing Fitbit physical activity dataset for assisting with NHS guidelines, underscoring the importance of balancing accessibility with privacy. Future research should focus on refining these mechanisms, considering diverse scenarios and personalized health data access, while maintaining privacy integrity. This work sets a foundation for safer and more efficient healthcare services, leveraging robotic assistance.

Acknowledgement

For purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising from this submission.

References

[1] F. Cavallo, R. Esposito, R. Limosani, A. Manzi, R. Bevilacqua, E. Felici, A. Di Nuovo, A. Cangelosi, F. Lattanzio, P. Dario, *et al.*, "Robotic services acceptance in smart environments with older adults: user satisfaction and acceptability study," *Journal of medical Internet research*, vol. 20, no. 9, p. e9460, 2018.

[2] A. Di Nuovo, F. Broz, N. Wang, T. Belpaeme, A. Cangelosi, R. Jones, R. Esposito, F. Cavallo, and P. Dario, "The multi-modal interface of robot-era multi-robot services tailored for the elderly," *Intelligent Service Robotics*, vol. 11, pp. 109–126, 2018.

[3] N. Camp, J. Johnston, M. G. Lewis, M. Zecca, A. Di Nuovo, K. Hunter, and D. Magistro, "Perceptions of in-home monitoring technology for activities of daily living: semistructured interview study with communitydwelling older adults," *JMIR aging*, vol. 5, no. 2, p. e33714, 2022.

[4] C. De Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, "Generic aaa architecture," tech. rep., 2000.

[5] G. Lopez, O. C´anovas, A. F. G´omez, J. D. Jim´enez, and R. Mar´´ın, "A network access control approach based on the aaa architecture and authorization attributes," *Journal of Network and Computer Applications*, vol. 30, no. 3, pp. 900–919, 2007.

[6] D. Golinelli, E. Boetto, G. Carullo, A. G. Nuzzolese, M. P. Landini, M. P. Fantini, *et al.*, "Adoption of digital technologies in health care during the covid-19 pandemic: systematic review of early scientific literature," *Journal of medical Internet research*, vol. 22, no. 11, p. e22280, 2020.

[7] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5453–5458, IEEE, 2006.

[8] C. Lutz, M. Schottler, and C. P. Hoffmann, "The privacy implications¨ of social robots: Scoping review and expert interviews," *Mobile Media & Communication*, vol. 7, no. 3, pp. 412–434, 2019.

[9] S. Bayreuther, F. Jacob, M. Grotz, R. Kartmann, F. Peller-Konrad, F. Paus, H. Hartenstein, and T. Asfour, "Bluesky: Combining task planning and activity-centric access control for assistive humanoid robots," in *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, pp. 185–194, 2022.

[10] J. Marchang and A. Di Nuovo, "Assistive multimodal robotic system (amrsys): security and privacy issues, challenges, and possible solutions," *Applied Sciences*, vol. 12, no. 4, p. 2174, 2022.

[11] NHS, "Physical activity guidelines for adults aged 19 to 64," 2023.

[12] R. Furberg, J. Brinton, M. Keating, and A. Ortiz, “Crowd-sourced fitbit datasets 03.12.2016-05.12.2016.” https://doi.org/10.5281/zenodo.53894, 2016.