2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) | 978-1-6654-0424-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/PERCOMWORKSHOPS51409.2021.9431036

A Policy-Based Approach for Managing Socially Appropriate Interaction Behaviours in IoT Collectives

Amna Batool, Seng W. Loke, Niroshinie Fernando and Jonathan Kua
School of Information Technology
Deakin University, Geelong, Australia
{abatool, seng.loke, niroshinie.fernando, jonathan.kua}@deakin.edu.au

***Abstract*—In this paper, we investigate a policy based approach for managing socially appropriate interaction behaviours in Internet of Things (IoT) Collectives, i.e., a collection of IoT devices. In particular, we consider scenarios in an aged care home environment. We have designed a policy management framework with three different types of rules - Authorisation, Obligation and Prohibition rules for smart internet-connected devices in an aged care centre where smart robots follow consensus-seeking processes while monitoring the elderly people. We consider the management of socially appropriate interaction behaviours in IoT devices based on a policy management framework and demonstrate its applicability with the system we prototyped called KATE.**

***Index Terms*—Policy, Policy management framework, socially appropriate behaviours, IoT Collectives, aged care centre**

I. Introduction

Internet of things (IoT) refers to a collection of technologies involving Internet-connected smart things, such as robots, smart cameras, sensors, etc. Interactions between a human and an object create a smart application experience in smart environments, but such smart objects need to behave ethically/appropriately while interacting with humans. In this context, we focus on a policy-based approach for managing socially appropriate interaction behaviours in IoT collectives, adopting a deontological approach, as a practical implementable approach. It is important to have rules applied on IoT devices during human-device interaction; therefore, we have designed three different types of rules to be applied on smart internet-connected IoT devices for managing the ethical actions (appropriate behaviours) appropriately in an aged care centre. Different smart devices might interpret ethical behaviours (in the form of a rule) differently, such as a smart camera can be "privacy-respecting" by not capturing private information including financial cards, identity cards etc, even when being instructed to do so. Similarly, a smart vacuum cleaner can "be polite" by using phrases such as "Hello" or "Excuse me" while cleaning different rooms, if the rule it is given is to "be polite". IoT devices have to be ethical during their actions as it is important to stay within the comfort zones of persons.

In this paper, we aim to design and use a policy-based approach for managing socially appropriate (and to an extent, ethical) interaction behaviours in smart robots in an aged care centre. Our policy management framework has authorisation, obligation and prohibition rules to be applied on IoT collectives where smart robots must follow obligation rules which are designed based on ethical actions. For example, we developed a system which we named KATE based on a scenario where a smart Internet-connected robot is placed in an aged care centre and it has to monitor the seniors. While monitoring the seniors, it is compulsory for the smart robot to trigger consensus-seeking processes when it interacts with seniors, for example, seeking approval before monitoring any senior, be polite while roaming around, or keeping the seniors informed of each action (so as not to startle or cause discomfort). If smart devices behave ethically, as appropriate, the usage of IoT can be increased in health care centres potentially.

Given that smart devices could potentially be used in future aged-care centres, it would be crucial that they take appropriate actions while interacting with the seniors - motivating the need for socially appropriate interaction behaviours in multiuser - multidevice interactions in IoT collectives. To realize consensus-seeking processes on smart devices, we have designed a system with actuator and mediator applications separating the concerns of taking action from parties that initiate or request these actions.

The rest of this paper is organised as follows. §2 provides the background of our work and reviews related work on socially appropriate interaction behaviours in smart devices. §3 presents our system architecture with policy management framework for IoT collectives. §4 presents the modelling of socially appropriate interaction behaviours in the KATE system, including its concept and system implementation. §5 concludes and discuss future work.

II. Background and Related Work

Elderly people in aged care centres can feel lonely and depressed which are of serious concern and due to which many of the countries are developing a new aged-care model where smart internet-connected devices can utilise to help seniors in living a healthy lifestyle [1]. There are different studies carried out on using particular smart devices especially robots to assist elderly people, e.g., [2], [3], [4]. It is also essential to maintain ethical actions in smart devices when they are used in an aged care home because some seniors may not be always comfortable in interacting with smart devices especially the robots [5]. In this context, elderly people need a wide range of communicating medium which interacts with them ethically and allows them to interact with their family and friends appropriately and they able to live a quality life.

There are various studies focusing on human-IoT interaction but not on interaction behaviours, especially socially appropriate interaction behaviour. Niemelä et.al [6] conducted a series of three different trials to determine how using a telepresence robot influences the seniors, family members and care workers at a residential care facility. The telepresence robots were installed at the facility to allow seniors to talk with their family members over a video call. Based on the outcomes of each trial, there were ethical issues that should be considered; e.g., seniors and family members had privacy as a huge concern. The participants commented that it is compulsory for a primary user to select with whom they are comfortable to talk with. Körtner et.al [7] illustrated the ethical issues in Henry - an autonomous and mobile robot platform which entertains elderly people by playing music and assist visitors at corridors to show them the particular office in an Austrian care institution.

Caine et. al [8] presented the effects on privacy-enhancing behaviours through an experimental study in which the seniors communicated with a camera, a stationary robot and a mobile robot. The cameras were installed all around the aged care centre and informed the seniors that they are being monitored all the time. The seniors were not comfortable in performing most of the activities including physical contact with a partner, doing some personal finances, having friends over, and so on, in front of the camera. Moreover, most of the elderly people tried to cover up the camera with an object and also tried to rotate it to a different direction away from them. Overall, the seniors had altered the way of performing most of their activities in front of the camera due to privacy concerns.

Krupp and Smart [9] arranged a focus group to discuss the privacy concerns about robotics technology. The main ideas covered in the discussion were about the physical, social and psychological privacy to be categorised properly in robotics technology as these are not well-categorized currently. In another study, Butler et.al [10] suggested reducing the quantity of visual information that smart teleoperated robots receive to preserve the end-user's privacy. They have explored different in-home privacy concerns including locations - where the robots should get access, the objects - which are accessible and which are not accessible, and finally the information, including identity cards, medical information and financial data, which need to be kept secured. The authors have proposed some image filters including Blur, Edge, Superpixel and colour-skewed superpixel for enhancing the privacy of the end-users. Hubers et. al [11] suggested video manipulations for remote presence systems to keep important data private. The authors have evaluated three observational privacy schemes, including "can't tell" which means not to include anything placed on a table or in a room, "can't observe" which means not to observe a particular shape of a person or object and "can't discern" which means not able to read information, for privacy protection in smart remote presence technology.

The above studies discussed the privacy concerns in IoT devices especially in robots, but did not implement the socially appropriate interaction behaviours in real-world scenarios based on multiuser and multidevice interactions in IoT Collectives. Moreover, the researchers have elaborated on the ethical issues and privacy enhancing behaviours in smart robots without proposing an appropriate approach for handling ethical issues in smart devices. It is crucial to maintain socially appropriate interaction behaviours in smart devices. The comfort zones of users need to be considered during human-device interaction. To this end, this paper proposes and designs a policy management framework for managing socially appropriate interaction behaviours in smart internet-connected devices based on multiuser-multidevice interactions in IoT collectives.

III. A System Architecture for Multiuser-Multidevice Interaction with a Policy Management Framework

Human-device interaction allows devices to perform different actions based on user request. In our research, we focus on interaction behaviours of smart devices where, the smart devices have to take multiple requests from multiple users and behave appropriately, handle uncertainty and make decisions. Fig. 1 presents the architecture of our system.

There are two types of applications i.e. *Actuator applications* (actuators) and *Mediator applications* (mediators). Actuator applications (which have to perform some actions) include IoT collectives which mean all smart devices such as smart robots, smart cameras, smart speaker et cetera. On the other hand, Mediator applications (communicating medium between user and actuators) include only mobile devices operated by users. There are some common services that can be performed by actuator and mediator applications on their own but the database is common in both ends. The actuator applications can monitor and assist users, store data in a database while the mediators can send multiple requests to actuators and retrieve data from the database. While monitoring or assisting users, it is compulsory for actuators to perform distributed services which are to behave appropriately, make smart decisions and handle task uncertainty. Lastly, the communication service can be managed through a WiFi network.

To be able to accomplish the research goal, we propose a policy management framework where the actuators and mediators have to follow the specific rules during human-device interactions. There are three rules designed for actuator and mediator applications. Fig. 2 presents the policy management framework.

- **Authorisation Rules:** The authorisation rules include monitoring as well as assisting users, sending multiple requests as well as retrieving data from the server

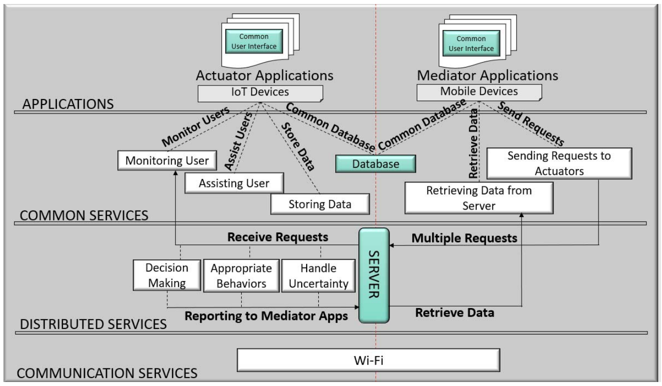

Fig. 1. Architecture of our system for multiuser-multidevice interaction behaviours in IoT collectives

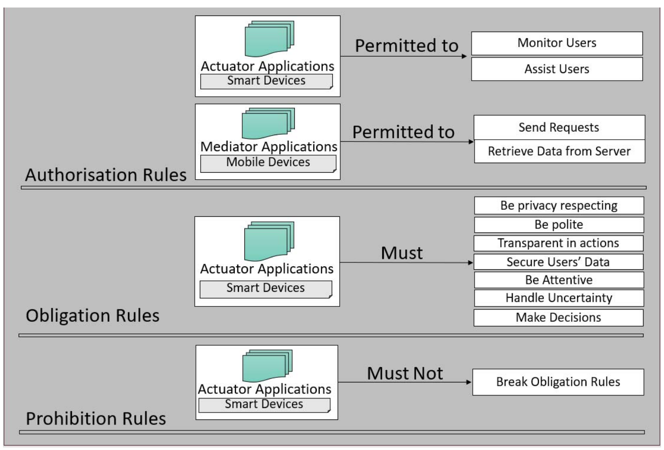

Fig. 2. Policy Management Framework with some examples of possible rules

which are permitted to perform by actuator and mediator applications. The actuator applications, including smart devices such as smart robots, smart cameras, or smart wheel-chairs, has to monitor and assist users on receiving requests from mediator applications. Monitoring or assisting users means to track the user's current situation and assist them in different activities.

For example, a smart robot in an aged care centre has to monitor the admitted senior after receiving a request from a family member of that senior through a mediator application (running on a mobile device). Similarly, the smart robot has to assist a carer staff member in their workload. In this way, smart robots are permitted to monitor and assist users. The mediator applications (mobile devices) are permitted to send requests to actuator applications as well as retrieve the data that actuator applications store on the server.

- **Obligation Rules:** The obligation rules are designed to be applied to actuator applications. Actuator applications must follow socially appropriate interaction behaviours i.e., be polite, privacy-respecting, secure users' data, transparent in all actions (e.g., reporting status) and so on, as well as handle tasks robustness and make decisions on multiple requests. For instance, if a smart robot is monitoring the senior in an aged care home then, it needs to be very polite, privacy-respecting, transparent in its actions and secure any data collected. Politeness in a smart robot could mean robots using phrases such as "Excuse me", "Hello", "May i have a way to pass" and so on, when appropriate as it performs its function in the aged care centre.
- **Prohibition Rules:** The prohibition rules are also designed to be applied to actuator applications only where, the actuator applications must not break the obligation rules, as one example, but other types of prohibitions can be considered - e.g., a robot is not allowed to take pictures or operate during particular times and so on.

Different IoT devices interpret obligation rules differently such as a smart wheel-chair can be polite by greeting users sitting on them as well as can ask if they are sitting comfortably. Similarly, a smart speaker can be polite by asking a user if they need to manage the sound level of a particular song. Likewise, a smart camera, when requested by a family member to do so, can seek approval of the senior before capturing the senior's photo, to be polite or privacy-respecting. In this paper, we have modelled obligation rules via a policy-based approach to manage ethical behaviours in smart robots in an aged care centre scenario which is further explained in section four.

IV. Our Prototype: KATE

Based on the conceptual design above, we describe our implementation of obligation rules to manage socially appropriate interaction behaviours in our KATE prototype system.

A. *KATE System: Concept*

KATE is a system comprising actuator applications (in particular a robot app running on a robot (we have used Temi robots[1]) and mediator applications (in our prototype, these are mobile apps running on smartphones of family members and caregivers). The actuators targeted in KATE system are smart internet-connected robots while mediators are mobile devices. The KATE system is designed and implemented for an aged care environment. The actuators have to monitor the seniors admitted in an aged care home and assist staff members to store medical data on the server to be accessible by family members of these seniors. The family members who have admitted their seniors in an aged care centre have to use a mediator application to send a request to the actuators to monitor the senior. Likewise, the staff members have to use mediator application to send a request to actuator to visit them and store senior's blood pressure and sugar level on the server. The family members can retrieve the monitored data from the server using the mediator application. While accomplishing families or staff member's requests, it is compulsory for actuators to behave ethically, able to handle task failures as well as make accurate decisions on which request must be completed at first.

[1]https://www.robotemi.com

KATE system has been designed and prototyped in this research - an early version without a policy framework was first proposed in press [12]. In this previous work, KATE is prototyped to show how complex interactions can be created in an aged care centre where the actuators are taking multiple requests from family members as well as staff members but are not following socially appropriate interaction behaviours including politeness, privacy-respecting, transparency in actions and so on. Expanding the KATE system in this paper, we are applying obligation rules from a policy management framework to manage socially appropriate interaction behaviours in smart robots while interacting with seniors or staff members in an aged care centre. Fig. 3 presents a picture of the whole scenario.

B. Application of Policy Rules on the KATE System

There are three types of rules in our policy management framework which have been applied to smart robots in an aged care centre as a case study. Each rule is applied and programmed into the system.

Authorisation Rules: The actuators (smart robots) and mediators (smart mobile devices) are permitted to follow authorisation rules which are: to monitor the users, assist the users, send multiple requests and retrieve monitored data. The actuators (smart robots) are permitted to monitor the seniors in an aged care centre and assist carer staff members on receiving requests from mediators; which are permitted to send requests to actuators as well as retrieve monitored data. Actuators are receiving multiple requests from mediators using a first come first serve queuing algorithm but the priority is given to family requests. The mediators and actuators are connected through a common database which is a firebase server. Using firebase database references, mediators send requests to actuators and actuators can accomplish those requests.

Obligation Rules: The actuators (smart robots) must follow the obligation rules (in order to behave ethical, using a narrow deontological definition of ethical in this case), handle task failures and make accurate decisions. The actuators must be ethical while interacting with seniors and carer staff members which means, actuators need to seek approval before taking any action, e.g. be privacy-respecting, and be polite while roaming around the aged care environment, be transparent of each action, secure senior's data and recognise a senior's face (to response accurately). Obligation rules for managing socially appropriate interaction behaviours in actuators (smart robots) are applied using different methods i.e., text to speech conversions, dialogue boxes, face recognition, firebase references, voice recordings, unique senior's IDs' and so on. The interpretation of ethical behaviours by smart robots in KATE system is explained in detail in the next sub-section.

Prohibition Rules: The actuators (smart robots) are prohibited from breaking the obligation rules assigned to them. The prohibition rules are applied to actuators (smart robots) using multiple conditions. For instance, if the mediator has to send a request to actuator then, the actuator must monitor the senior following the obligation rules.

C. Interpretation of obligation rules by smart robots in KATE system: System Implementation

Each device in an IoT Collective (or a collection of smart internet-connected devices) might interpret obligation rules differently. In our case, we are applying obligation rules to manage ethical behaviours in smart robots in an aged care centre. During an interaction with seniors, smart robots are interpreting the obligation rules explained below:

Privacy Respecting: The smart internet-connected robots are seeking approval from seniors before monitoring them. For instance, if the robot is asked by a family member via a mediator app to take a seniors' (called Senior, say) photo then, it first requests the Senior's permission by saying "Do You allow me to take your photo? Please respond to me using a dialogue box appearing on my screen". If senior response "Yes", then only the robot takes a photo and uploads it to a real-time database. Likewise, if senior allows the robot to ask daily routine questions in a similar way, then only the robot starts to ask the questions and records senior's answers as "voice notes" in a database. Smart robots are interpreting this rule by operationalizing it using text to speech conversation, dialogue boxes and voice recordings.

Transparency: The smart robots are letting seniors know about their actions - e.g. if senior has allowed them earlier to take a photo or ask routine questions through phrases "Thank You! I am going to take your photo", "Thank You! I am going to ask you some questions". Likewise, robots are letting family members be aware of each response from seniors provided on each request. For example, on one hand, if senior has denied the robot to monitor them, the robot reports back to the family by sending a message that "Your senior does not want me to monitor him/her at the moment". On the other hand, if senior has given them permission to monitor him/her, again the robot informs family members after completing the request so that the family member can retrieve the data (Senior's photo and voice notes) from the database. Transparency in action is interpreted by the robot to mean reporting to the family on each action or request status.

Politeness: The smart robots are very polite while roaming in an aged care centre. These smart robots are using phrases such as "Excuse me", "May I have a way to move" while moving around. If there is any object around, smart robots are using sensors to detect them and change their path followed by polite phrases.

Privacy of Data: The smart robots have to take Senior's photos as well as ask some routine questions to record and store them in a database. This data is fully secured as the robot is storing the files under each senior's ID that is only accessible to particular family members. Even the carer members can not access any photo or senior's voice notes on routine questions.

Attentive: Smart robots are recognising the senior's face on arrival, and then start monitoring them after seeking approvals. This rule is interpreted by robots using face recognition to focus on the right Senior (in this sense, to have attention focused on that individual). The seniors' photos are stored

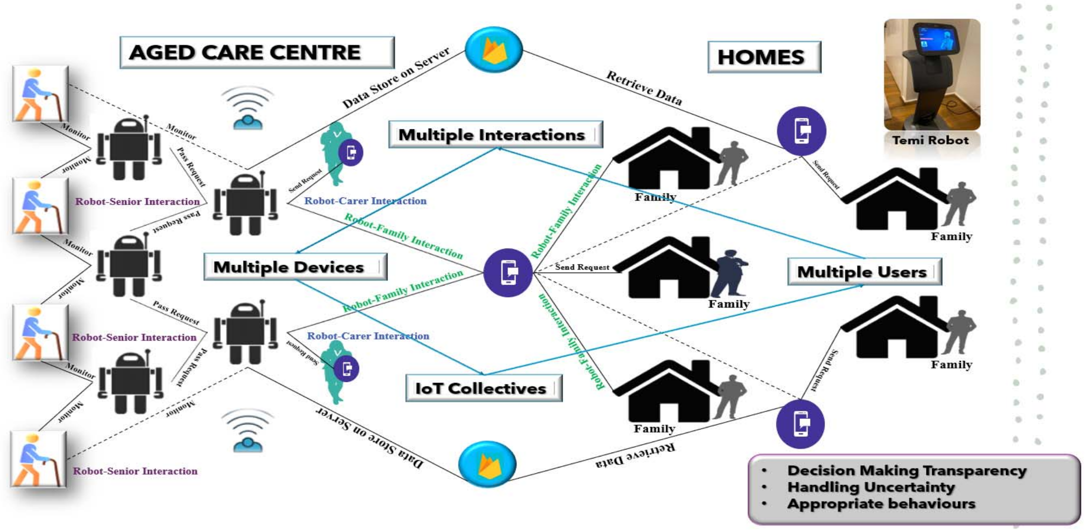

Fig. 3. KATE System

in the robot's memory and linked with each senior's name and ID so that when the robot arrives at a senior's location to monitor them, it can detect if this is the senior it has to monitor and then proceed accordingly.

Another aspect in our KATE system is that smart robots cannot move unless they are requested to do so - e.g., the family members send them a request to monitor a particular senior. Our system is not on auto-mode where smart robots can reach seniors anytime and start monitoring them. A video of KATE in operation (in a mock-up scenario) is available.[2]

D. State Transitions in KATE System based on multiuser-multidevice interactions

In the KATE system, We have multiple interactions such as robot-family interaction, robot-senior interaction and robot-carer interaction. During Robot-Family interaction, family members send a request to robot using mediator applications to monitor their senior in an aged care center, and robot is following socially appropriate interaction behaviours while monitoring the seniors therefore, it is compulsory to present the states and actions of smart internet-connected robots while completing requests appropriately.

Robot States and Actions during Robot-Family Interaction Fig. 4 presents the states and actions of the robot during robot-family interaction. The *robot activating* state will start on receiving a request from a family member that will allow the robot to examine the requests in the queue at *examining request* state. If it is a family request, the robot will start executing it in the *processing family request* state else, if it is a carer request, the robot will start executing it in the *carer request executing* state. To execute a request from a family member, the robot will start moving to the senior's location, where a condition is set which is, if senior is not located then, the robot will report to the family at *Reporting family* state that it is unable to find his/her senior, therefore, a family can send a request again after some time.

After reporting to family, the robot has to come back to the *Examining Request* state to look for the next request and start executing it. On the other hand, if robot finds the senior, it will start recognising h/her face in the *Face Recognising* state after which, again a condition is set which is, if in case it is not the Senior's face of whom the robot has to monitor, then it will again report to the family in the *Reporting Family* state and will come back to the *Examining Request* state to start the next request from the queue. Otherwise, if the robot successfully recognises the senior's face, it will seek approval in the *Seeking Approval* state before monitoring the senior. Here, we have another condition which is, if senior does not give the permission, then the robot will not disturb the senior and reports this to the family in the *Reporting Family* state and starts executing the next request, returning to the *Examining Request* state. In case the senior gives permission, the robot will start monitoring the senior in the *Questioning Senior* state and then will wait to get the answers from the senior in the *Waiting for Senior Answers* state. Once senior will respond to all queries, *Processing Senior Answers* state will start where the robot will able to process the answers. Finally, (super-)state *Store* will begin, where the robot will store the data on the real-time database and report to the family about request completion in the *Reporting Family* state again so that the family can retrieve the data. Finally, after reporting to family, the robot will come back to the *Examining Request* state to execute the next request. In this way, the process will continue and no disturbance will be created during interactions.

V. Conclusion and Future Work

Our policy-based approach for managing socially appropriate interaction behaviours in IoT collectives is of a high level of abstraction. We have designed a policy management framework including different rules to be applied on IoT

[2]See https://www.youtube.com/watch?v=K1j0fkvIaxY&t

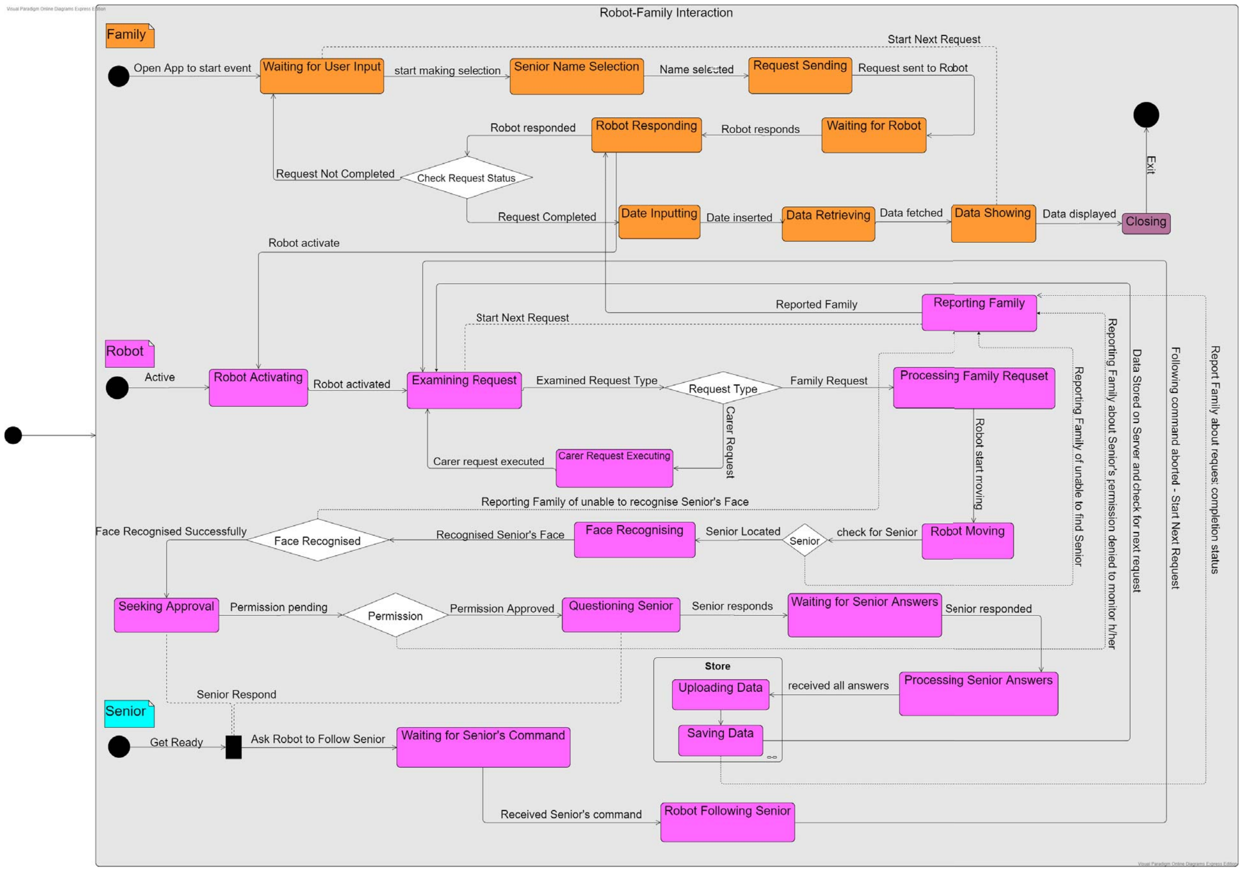

Fig. 4. Robot-Family Interactions

collectives to manage different behaviours. Different devices interpret these rules differently as we illustrated above. For example, the vision is that the manager of the aged care can just tell all the smart devices in the IoT collective in the aged care to "be polite" and each device will interpret this as appropriate to its own functions.

Implementation of ethical actions is highly beneficial but there is a need to think of some further interaction behaviours to include such as decision making and handling uncertainty. The KATE system will be extended to support such features.
Acknowledgment We acknowledge the support of Mr Yousaff Nawaz, CASE University Islamabad, in this project.

References

[1] Abir K Bekhet and Jaclene A Zauszniewski. Mental health of elders in retirement communities: Is loneliness a key factor? *Archives of psychiatric nursing*, 26(3):214–224, 2012.

[2] Rajiv Khosla, Khanh Nguyen, and Mei-Tai Chu. Human robot engagement and acceptability in residential aged care. *International Journal of Human–Computer Interaction*, 33(6):510–522, 2017.

[3] Lara Lammer, Andreas Huber, Astrid Weiss, and Markus Vincze. Mutual care : How older adults react when they should help their care robot. 2014.

[4] Masaaki Tanaka, Akira Ishii, Emi Yamano, Hiroki Ogikubo, Masatsugu Okazaki, Kazuro Kamimura, Yasuharu Konishi, Shigeru Emoto, and Yasuyoshi Watanabe. Effect of a human-type communication robot on cognitive function in elderly women living alone, 2012.

[5] Rosalie H. Wang, Aishwarya Sudhama, Momotaz Begum, Rajibul Huq, and Alex Mihailidis. Robots to assist daily activities: views of older adults with alzheimer's disease and their caregivers. *International psychogeriatrics*, 29 1:67–79, 2017.

[6] Marketta Niemelä, Lina Van Aerschot, Antti Tammela, Iina Aaltonen, and Hanna Lammi. Towards ethical guidelines of using telepresence robots in residential care. *International Journal of Social Robotics*, pages 1–9, 2019.

[7] Tobias Körtner. Ethical challenges in the use of social service robots for elderly people. *Zeitschrift für Gerontologie und Geriatrie*, 49(4):303–307, 2016.

[8] Kelly Caine, Selma Šabanovic, and Mary Carter. The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults. In *Proceedings of the seventh annual ACM/IEEE international conference on Human-Robot Interaction*, pages 343–350, 2012.

[9] Margaret M Krupp, Matthew Rueben, Cindy M Grimm, and William D Smart. A focus group study of privacy concerns about telepresence robots. In *2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*, pages 1451–1458. IEEE, 2017.

[10] Daniel J Butler, Justin Huang, Franziska Roesner, and Maya Cakmak. The privacy-utility tradeoff for remotely teleoperated robots. In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction*, pages 27–34, 2015.

[11] Alexander Hubers, Emily Andrulis, Levi Scott, Tanner Stirrat, Ruonan Zhang, Ross Sowell, Matthew Rueben, Cindy M Grimm, and William D Smart. Using video manipulation to protect privacy in remote presence systems. In *International Conference on Social Robotics*, pages 245–254. Springer, 2015.

[12] Amna Batool, Seng W.Loke, Niroshinie Fernando, and Jonathan Kua. Towards a system for aged care centres based on multiuser–multidevice interactions in iot collectives. EAI Mobiquitous, 2020.