2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)

A Methodology for Human-Centred IoT Collectives Based On Socio-Ethical Policies

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*—An emerging aspect to consider during human-device interaction is addressing ethical concerns about smart, internet-connected devices and making them behave in a more human-centred manner, i.e., ethically and in a socially acceptable manner. We propose that smart devices can be made to behave in a more human-centred manner, by the application of a set of policies to their fundamental operations, if a technique for defining their key roles and mapping ethical and administrative policies to them is developed. This paper proposes a methodology which consists of four primary phases, including concept development, defining and mapping policies, implementing the processing of policies and deploying the devices. Our suggested methodology may be used in a variety of situations where smart devices interact with people. For illustration, we have applied the proposed methodology to a supermarket scenario where each phase defined in the methodology has been followed.**

***Index Terms*—methodology, socio-ethical policies, IoT collectives, human-centred IoT**

I. Introduction

The Internet of Things (IoT) can be defined as a network of Internet-connected objects, or 'smart devices' with computing, sensing and/or actuating capabilities. The usage of these smart devices within diverse contexts such as smart homes, supermarkets, farms, hospitals and aged-care settings are increasingly becoming popular. In such environments, multiple users can use smart devices to interact with collections of other smart devices (e.g. family members living in a smart home). In our work, we use the term *IoT collectives* to refer to such systems [1]. IoT collectives can support ecosystems consisting of different users and devices such as smartphones, robots, drones and wearable devices to interact and work together. However, managing the interaction behaviours of a collection of heterogeneous devices, and ensuring responsible conduct, in a human-centric way remains a challenge. Consider a store with several robots and human customers, where a robot approaches people and begins photographing them without their consent. When the robot engaged with the user in this scenario, it executed its core functions without the user's permission. Is it appropriate for a robot to behave in this manner?

Our work focuses on controlling the interaction behaviours of such smart devices that are capable of performing autonomous functions. To do so, our approach is to identify the primary functions performed by smart devices, then map those functions to applicable socio-ethical and administrative policy rules, and finally embed the policy rules onto these devices, to operationalize the behaviour of smart devices. To this end, for developing an application that involves multiple IoT devices, i.e., involving what we call IoT collectives, this paper's main contribution is to propose a methodology that consists of four phases to guide developers, throughout the design and development process, in thinking about the desired socio-ethical behaviours of IoT devices and the corresponding socio-ethical policy rules that represent those desired socio-ethical behaviours.

Authorization, obligation, and prohibition rules are the three types of rules that govern the behaviour of smart devices in socio-ethical and administrative policies [1]. These rules are intended to apply to a variety of smart devices in IoT collectives. The socio-ethical policy rules are intended to be applicable across many domains, such as supermarkets, education centres, and elderly care facilities, while the administrative policy rules are particular to the environment. Each rule under socio-ethical and administrative policy is spelled-out explicitly in the XML language to make the rules operationalized by smart devices. There are three policy language documents that have been designed to be processed by IoT devices to learn what policies to follow and how to interpret each policy rule while doing their respective core operations.

We contend that our approach encourages a separation of concerns when thinking about IoT collectives - we first identify core functions of IoT devices as one concern, and then, the socio-ethical aspects as another concern, i.e. we identify the associated authorisations/prohibitions and obligations that would be associated with these core functions. We have applied our proposed methodology to a supermarket scenario where we have outlined an environment of a prototypical futuristic supermarket with installed multiple smart devices. This is explained in detail later in this paper.

How to embed AI ethical concepts into device software is now a hot topic [2]. Our suggested approach is a means to incorporate ethics into smart devices through defined socio-ethical rules and make them act ethically, which contributes an approach (albeit a pragmatic and computational one) towards addressing this issue. Software developers will benefit from the methodology because they will be able to create human-centric smart devices that conduct operations ethically. Normally, software developers use software engineering approaches to create software for a specific device, but our methodology will

978-1-6654-3583-3/21/$31.00 ©2021 IEEE
DOI 10.1109/ASEW52652.2021.00042

let them create ethical devices that act correctly in different situations.

The rest of this paper is organised as follows. §2 presents the background and related work. §3 presents the reference architecture. §4 presents an overview of the methodology for human-centred IoT Collectives. §5 presents the application of our proposed methodology to the supermarket scenario. §6 concludes with a discussion on future work.

II. Background and Related Work

Smart devices are utilised to generate human-device interaction, but little effort has been made to make these devices behave socio-ethically. Different approaches for making AI responsible have been presented in the literature, but they are primarily centred on single smart devices, not IoT collectives.

Dylan and Aimee [3] proposed an ethical framework to make the design, development, deployment, and evaluation of drones in public healthcare more efficient. The framework is founded on ethical concepts such as beneficence, non-maleficence, autonomy, and fairness, as well as comprehensibility. The ethical framework of the study connects abstract ethical concepts to human values, and then connects them to design needs through a translation process using contextual norms. Unfortunately, the study only targeted drones in healthcare centers, whereas, our study has proposed a methodology which is applicable to multiple smart devices in multiple domains, not only healthcare centers. Another approach is used in [4] which is the value-sensitive design method to solve an engineering design challenge involving the creation of a command and control supervisory display for the Tactical Tomahawk missile. VSD is an engineering education tool that bridges the gap between design and ethics for many engineering disciplines. Although VSD is highly recommended in engineering, it does not commit to a certain ethical framework/theory [5].

Liming et al. [2] looked at three challenges linked to human and AI interaction, which are hard-to-implement ethical AI principles, the generic idea of trust versus trustworthiness, and product/process support for trust/trustworthiness. In the context of AI ethical principles and responsible AI, the study highlighted the missing components in operationalising ethical AI concepts and potential solutions by utilising the example of agricultural yield prediction. However, aside from trust and trustworthiness, the study did not address the various aspects of ethical standards. Our methodological approach involves a phase of mapping socio-ethical policies, which include authorisation, obligation, and prohibition rules, to the fundamental tasks of devices in order to make them behave responsibly (or socio-ethically). Furthermore, our methodology enables the operationalization of ethical smart device behaviour using policies. Also, our approach does not address ethical AI in general, but specifically, smart devices (which might have embedded AI functionality).

It is essential that several strategies or approaches be considered in order to make smart devices responsible or ethical, but it is also necessary to examine smart device behaviour in many fields. Numerous studies in the literature have concentrated on the design of smart devices for usage in various domains or making them interact with humans in healthcare settings [6], [7], [8], but none have focused on device behaviour.

Yamato et al. [9] addressed the use of assistance robots by elderly people in supermarkets. The research team created two types of robots: a cart robot that can carry items and a conversational robot that can speak with elderly people as they shop. Twenty-four older citizens were invited to engage with robots at a supermarket as part of an experiment. Both robotic designs were approved by the seniors, but they preferred the talking one. The study focused on the design of robots rather than on their ethical behaviour with the elderly. Our study focuses on controlling the behaviour of smart devices through policies imposed on them using our methodological approach. M.G. Sarwar et al. [10] introduced the EdgeLite concept, which enables smart devices to identify and react to hazards on supermarket floors in real time. The researchers created real-world collection of pictures depicting dangers on store floors. This collection includes pictures of supermarkets that have been classified as having a dangerous floor and not. Our work focuses on controlling devices in environments, e.g., in supermarkets using policies.

You and Chang [11] presented a 3S-cart sensor-based supermarket cart for smart shopping. The 3S-cart can track the actions of its users and respond accordingly. Customers can utilise the LCD screen on the sensor-based cart to request product details, or the 3S-cart can monitor user behaviour and automatically show item data on the screen. The sensor-based cart is an IoT-based project, and while it's fascinating to observe how it detects users' behaviour, our research is focused on device behaviour towards people.

In the literature, various approaches to making smart devices responsible have been explored, and only a few have discussed the integration of ethics in IoT, and do so without providing an effective computational solution/approach. Our proposed methodology can be used to operationalize ethical behaviour in the Internet of Things by enacting policies that govern smart device interaction. Using smart devices in various areas is useful, but maintaining control over device behaviour is equally important. Our approach also enables devices to interact with people in a socially appropriate manner. The stages of the methodology are detailed later in this work.

III. Reference Architecture

Our proposed methodology relates to IoT devices explicitly represented in our designed reference architecture. Figure 1 presents the reference architecture consisting of four layers: end-user layer, processing layer, network layer, and actuator layer. The mediator and administrator applications that operate on communicating and admin devices, respectively, make up the end-user layer. The communicating devices are those that allow users to engage with actuators (which are IoT devices), while the admin devices are those that allow facility managers to enforce administrative policy rules on IoT devices. Some of the examples of communicating and admin

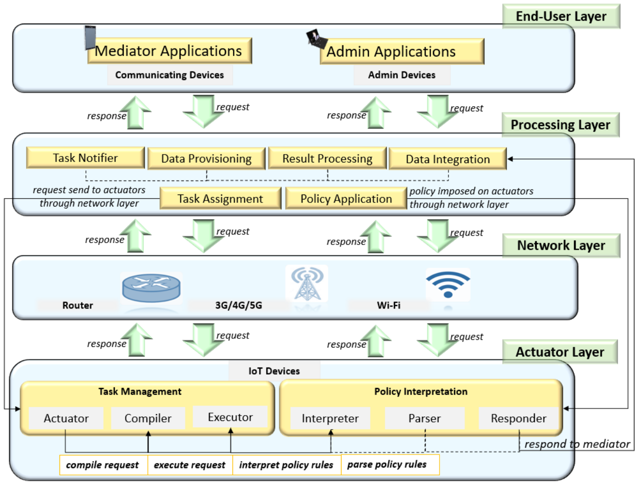

Fig. 1. Reference architecture represents devices: communicating devices, admin devices, and IoT devices.

devices are smartphones, laptops, desktops, tablets, and so on. The communicating devices and admin devices connect with actuators through the processing and networking layers. In the processing layer, the tasks and policies to be imposed on IoT devices generated by communicating and admin devices are handled. The tasks and policies are transferred to the Actuator layer through Wi-Fi, 3G/4G/5G, or routers, which are network layer components, once they have been processed. The IoT devices/Actuators compile and perform the job once it reaches the Actuator layer. They use the interpreter component to see if the admin has imposed policy rules on an intended task. When the actuators have completed their tasks, they communicate with the communication and admin devices via the network layer. The data that communicating and admin devices receive from actuator devices or actuator devices receive from communicating and admin devices is combined, processed, and then sent to them through a task notifier as shown in processing layer. In this manner, mediators and administrators send requests to actuators, while actuators provide replies back to mediators and administrators through the network and processing layers.

IV. Development Methodology for Human-Centred IoT Collectives

The methodology described in this paper aims to help developers make smart devices more human-centric by managing their interaction behaviour through the application of policies to them. Each stage of our recommended methodology is linked to the software engineering methodology approach. The first stage of our methodology, concept development, is similarly related to the first phase of a software methodology, requirements gathering. Similarly, the second stage, i.e., define and map policies, corresponds to both the software engineering methodology's requirements and design phase. Furthermore, the third stage concerns how to process policies, which corresponds to a typical software engineering approach's implementation phase, and the fourth phase, install and deploy, is related to the software engineering methodology's deployment and testing phase. Each phase of the methodology is iterate-able. Figure 2 presents our methodology consists of four phases, which are detailed below:

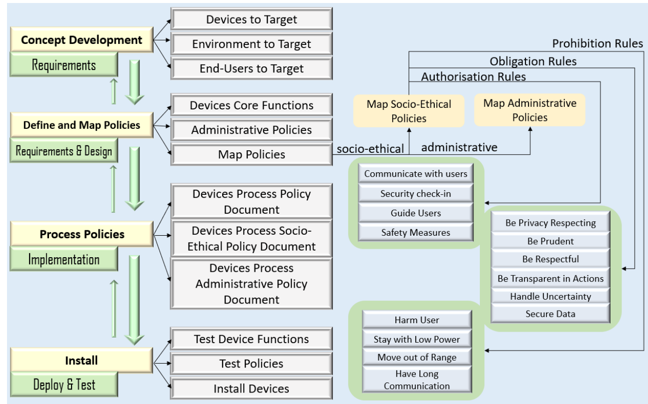

Fig. 2. Policy Development Methodology for IoT Collectives

Concept Development: The smart devices to target, in the IoT collective, are listed in the first phase, along with the environment in which these devices must be utilised. Furthermore, the end-users with whom the targeted smart devices will interact are also listed in this phase. For example, if smart cameras and robots are to be deployed in a supermarket setting, this must be detailed at this stage. Furthermore, if robots must interact with customers and cameras with employees, this stage classifies all end-users with whom the devices will interact.

Define and Map Policies: Smart devices carry out their primary functions but might do so in a purely functional and direct manner. For example, a robot needs to converse with humans, however unless thought through by developers about appropriate ways to converse, robots will not demonstrate politeness when conversing with humans. As a result, it is important to understand a device's core behaviours in order to augment the core behaviours with policy-rule behaviours causing the device to act appropriately even while performing its core activities. The main activities performed by each targeted IoT device must be identified and specified in this phase. The administrative policy rules must be defined after the core functions (or behaviours) of each smart device has been determined.

For example, what authorisation, obligation, and prohibition rules under an administrative policy are necessary if a robot is to execute its basic job of keeping track of products on a supermarket shelf? Socio-ethical policy rules are pre-defined as shown in Figure 2 because these rules are required to make a device behave in an ethical manner - in our methodology, we predefine a set of socio-ethical policy rules, one or more of which might be applicable to a given application.

Administrative rules, on the other hand, must be specified in order to regulate smart devices' environment-specific behaviours. Once the administrative policy rules are defined, the socio-ethical and administrative policies need to be mapped to each defined core function of the device.

Both socio-ethical and administrative policies comprise authorisation, obligation, and prohibition rules, as stated in section one. As a result, each core function will be mapped to the policies' particular authorisation, obligation, and prohibition rules. The idea is that the designer thinks about and writes out not only each device's core functions/behaviours, but also the corresponding applicable policy rules that relate to the device's socio-ethical aspects (i.e., the device's authorisations/prohibitions and obligations) while performing core functions.

Process Policies: Three policy documents must be loaded onto smart devices in this phase, since they contain the policy rules to operationalize the authorisations/prohibitions and obligations mapped to the devices' core functions/behaviours. The first document explains what policy rules a device has to follow, while the second and third documents explain how to interpret the socio-ethical and administrative policy rules, respectively. When each document is placed on smart devices, they will be able to learn what rules to follow and how to interpret each rule while carrying out their primary job. Note that we define what rules each device has to follow separately from how an applicable rule is interpreted by a device since two devices might interpret the same policy rule differently, depending on their core functions and capabilities.

Install: The final phase is to put each device into the environment after loading policy documents. If a robot is to be placed in a supermarket, for example, once the robot's basic functions have been defined, policies have been mapped to each core function, and policy language documents have been embedded in the robot, it is finally ready to begin operation.

Each stage of our proposed methodology aids in the deployment of smart devices that have socially appropriate interaction behaviours. The behaviour of the devices prior to the application of policies is only a core function that they execute (which can be an absence of acceptable behaviour). The devices' behaviour becomes ethical and controlled after mapping socio-ethical and administrative policies to the devices' core functions and embedding them with policy rules to operationalize the right socio-ethical behaviours. In the next section, we discussed how we applied our methodology to a supermarket scenario.

V. Application of Our Methodology to a Supermarket Scenario

Multiple smart devices, particularly robots, are being used in various areas without consideration for the regulation of their interaction behaviour [6] [7] [8]. We previously used our policy-based approach on robots to govern their interaction behaviours in a scenario of an elderly care facility [1] [12], though without an elaboration of the methodology we are proposing in this paper. As an illustration of our methodology, we apply it to a supermarket scenario here.

Fig. 3. Supermarket Domain showing an IoT collective consisting of multiple robots, smart cameras, smart speakers with customers and employees.

A. Supermarket Scenario: Concept

Figure 3 illustrates the whole supermarket scenario, in which a variety of smart devices, such as robots, smart cameras, and smart speakers, must be placed to execute their primary functions. According to the scenario, three robots must be placed throughout the market to execute various tasks. One of the robots is in charge of keeping track of the shelves, keeping an eye on customers, and detecting rubbish on the floor. The second robot is responsible for recognising staff members' faces at the main door for attendance purposes, as well as delivering online-ordered products to automobiles parked outside the market. The third robot is responsible for assisting customers and directing them to various shop areas. On the other hand, two smart cameras must be put on the market. One on the wall to keep an eye on the surrounds, and one at the main entrance to stream live for security purposes. Finally, numerous smart speakers must be put at various shop locations to allow customers to scan the product bar-code and obtain a description of the item. Following the methodological phases, the devices must perform activities adhering to policies that must be mapped to their core functions. Furthermore, devices will learn how to interpret each policy through policy documents.

B. Methodology's Applicability

Each phase of our proposed methodology has been tested on the supermarket scenario explained in the last sub-section. The phases are described below:

Concept Development: Following the first phase of the methodology, the following are the smart devices that are being targeted in the supermarket scenario:

- Actuators (IoT devices): robots, smart cameras, smart speakers
- Mediators (Communicating Devices): smartphones and tablets

- Administrator (Admin Devices): smartphones and tablets

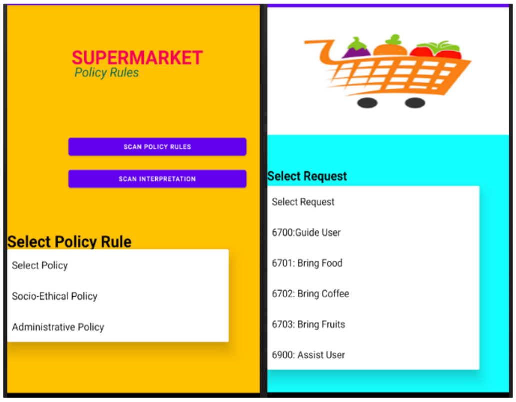

Fig. 4. Administrator App (Left), Mediator App (Right)

The robots are using launcher OS 1337 and software version 120.07. Android OS is used in the smart speakers and smart cameras. Similarly, Android OS is used on mediator and administrator devices. Figure 4 shows the mediator application's interface, which users may utilise to interact with the robot and the administrator's application interface, which the admin may use to enforce administrative regulations on smart devices. The supermarket is the environment in which the smart devices must be installed, and the end-users with whom the devices will interact include customers, employees, and administrators.

Define and Map Policies: Following the second phase of the methodology, Table I displays the primary functions performed by each device in terms of supermarket environment. The next step in this phase is to define administrative policies after each smart device's primary function has been specified. Table II and Table III outlines the socio-ethical policies and administrative policies mapped to the devices' core functions.

Process Policies: Following the third phase, the policy language documents are created independently for each targeted smart device. As a result, each device must load its three policy documents in order to understand what policy rules it must obey and how to interpret each socio-ethical and administrative policies while executing its core functions. For instance, if a robot has a core function of taking users to different locations, then the authorisation rule that applies to its core function is "guide-user". While guiding, the obligation rules that apply to robots are to "be-respectful", which means being polite with the users, "be-transparent-in-action", which means informing the users of the location where they are being directed by the robot, and "handle-uncertainty", which means avoiding obstacles or finding alternate paths in crowded areas. The prohibition applies is "moving out of range" (i.e., it should not move out of range) under the socio-ethical policy. The robot must know how to interpret these rules while guiding the user. Therefore, it is essential to load policy documents onto robots to let them understand the interpretation of each rule through our designed policy language documents.[1]

TABLE I
PRIMARY FUNCTIONS OF SMART DEVICES

Smart Devices	Primary Functions
Robot	Interact with customers as they enter the store to see whether they require assistance Recognise staff members' faces to record their attendance Take customers to various shop locations in order to direct them to the products on the shelves Detect litter/trash on the floor to prevent customers from slipping and getting hurt Display item details to customers to let them know the item price, expiry date, ingredients, and so on Keeps track of products on shelves and alerts employees if an empty shelf or low item quantity is discovered Deliver online-ordered products to cars parked outside the store Keeps an eye on the customers to make sure everything is in order
Smart Camera	For security reasons, record footage of the surroundings Display videos to the administration to keep track on security Detect dangers by streaming the environment in real time Recognize the faces of employees and customers for safety reasons Scan product bar-codes to keep track of items Alert about hazards to customers and staff Look after the customers to make sure everything is good around
Smart Speaker	Display product prices to customers Play music in cafe areas for visitors Tell jokes in cafe areas for entertainment purposes Detect staff members' voice for security purposes Alert about hazards to customers and staff Scan product bar-codes to keep track of items

Install: In this phase, each targeted device has to be installed in the supermarket. Figure 5 shows a robot taking a user's guide-me request. When the robot receives the request, it goes to the spot where the user is and guides the user to where s/he wishes to go. Socio-ethical policies mapped to device fundamental functions work across domains, which implies that while a robot is guiding or aiding humans, it must follow socio-ethical policies, but administrative policies must be relevant to the environment. As a result, the administrator has the ability to enforce administrative policy rules on smart devices. The smart devices must obey all policy rules that apply to their fundamental functionality when executing these activities. In terms of obligation rules, a smart camera, for example, is required to protect users' privacy while viewing the surroundings, and it is not permitted to continue working if its power falls below the threshold in terms of prohibition rules under the socio-ethical policy. Similarly, the smart speaker is required to maintain loudness under administrative policy's obligation rules and is not permitted to disturb customers needlessly under administrative policy's prohibition rules.

Overall, we contend that it is highly beneficial to deploy IoT devices in various contexts while maintaining control over their interaction behaviour. The methodology was successfully applied to the supermarket situation, illustrating core functions and associated socio-ethical policies.

[1]The full document on robot socio-ethical policy is available: https://github.com/abatool-abatool/POLICY-LANGUAGE-SUPERMARKET-DOMAIN/blob/main/Socio-Ethical-Robot-Supermarket. Similarly, the complete document for the socio-ethical policy of smart cameras is available: https://github.com/abatool-abatool/POLICY-LANGUAGE-SUPERMARKET-DOMAIN/blob/main/Socio-Ethical-Camera-Supermarket, and the smart speaker socio-ethical policy document is available: https://github.com/abatool-abatool/POLICY-LANGUAGE-SUPERMARKET-DOMAIN/blob/main/Socio-Ethical-Speaker-Supermarket. The full document of the robot administrative policy is available: https://github.com/abatool-abatool/POLICY-LANGUAGE-SUPERMARKET-DOMAIN/blob/main/Administrative-Robot-Supermarket. Similarly, the complete document of the administrative policy for the smart camera is available: https://github.com/abatool-abatool/POLICY-LANGUAGE-SUPERMARKET-DOMAIN/blob/main/Administrative-Camera-Supermarket and the smart speaker's administrative policy document is available:https://github.com/abatool-abatool/POLICY-LANGUAGE-SUPERMARKET-DOMAIN/blob/main/Administrative-Speaker-Supermarket

TABLE II
SOCIO-ETHICAL POLICIES AND CORE FUNCTIONS MAPPING

Smart Devices	Core Function	Authorisation	Obligation	Prohibition
Robot	Interacting with users	Communicate-with-Users	Be-Respectful Be-Transparent-in-Actions	Harm-User Stay-With-Low-power
	Recognise users' face	Security-Check-In	Be-Privacy-Respecting Be-Prudent Secure-Data Be-Transparent-in-Actions	Harm-User Stay-With-Low-power
	Take users to different locations	Guide-Users	Handle-Uncertainty Be-Respectful Be-Transparent-in-Actions	Move-Out-of-Range Stay-With-Low-Power Have-Long-Communication
	Detects trash on floor	Safety-Measures	Be-Respectful Handle-Uncertainty	Harm-User Move-Out-of-Range Stay-With-Low-power
Smart Camera	Capture videos/photos	Safety-Measures	Be-Privacy-Respecting Be-Transparent-in-Actions Handle-Task-Failure	Harm-Users Move-Out-of-Range Stay-With-Low-Power Have-Long-Communication
	Display video/photo	Communicate-with-Users	Be-Respectful Transparent-in-Actions Secure-Data Handle-Task-Failure	Stay-With-Low-Power Have-Long-Communication Harm-Users
	Stream live	Safety-Measures	Be-Privacy-Respecting Be-Transparent-in-Actions Be-Prudent Handle-Task-Failure	Harm-Users Move-Out-of-Range Stay-With-Low-Power Have-Long-Communication
	Detect user's face	Security-Check-In	Be-Respectful Be-Prudent Secure-Data Be-Transparent-in-Actions	Stay-With-Low-power Harm-Users
Smart Speaker	Playing music	Guide-Users Safety-Measures	Be-Privacy-Respecting Be-Transparent-in-Actions Handle-Task-Failure Be-Prudent	Harm-Users Move-Out-of-Range Stay-With-Low-Power Have-Long-Communication
	Telling jokes	Communicate-with-Users Safety-Measures	Be-Respectful Be-Transparent-in-Actions Handle-Task-Failure	Harm-Users Stay-With-Low-Power Have-Long-Communication
	Detect users' voice	Security-Check-In	Be-Respectful Be-Prudent Secure-Data Be-Transparent-in-Actions	Stay-With-Low-power Harm-Users
	Display product prices	Communicate-with-Users	Be-Respectful Be-Transparent-in-Actions	Harm-Users Stay-With-Low-Power Have-Long-Communication

TABLE III
ADMINISTRATIVE POLICY RULES AND CORE FUNCTIONS MAPPING

Smart Devices	Core Function	Authorisation	Obligation	Prohibition
Robot	Overlook users	Observe-User	Protect-Self Be-Prompt-In-Actions Alert-To-Fire-Alarms	Enter-Private-Locations Talk-To-Strangers
	Display item details to user	Assist-User Enlist-Product-Prices	Maintain-Volume Be-Prompt-In-Actions Protect-Self	Enter-Private-Locations Talk-To-Strangers Disturb-Unnecessarily
	Keep track of products in shelves	Monitor-Shelves	Maintain-Volume Be-Prompt-In-Actions	Enter-Private-Locations Talk-To-Strangers
	Manage Electronic Shopping	Manage-Online-Orders	Maintain-Volume Be-Attentive	Talk-To-Strangers Disturb- Unnecessarily Enter-Private-Locations
Smart Camera	Overlook users	Observe-User	Maintain-Volume Be-Prompt-In-Actions	Talk-To-Strangers
	Scan barcodes	Assist-User Enlist-Product-Prices	Maintain-Volume	Talk-To-Strangers Disturb- Unnecessarily
	Detect user's face	Observe-User	Maintain-Volume Be-Prompt-In-Actions Be-Attentive	Talk-To-Strangers Disturb- Unnecessarily
	Alert on hazard	Assist-User	Alert-To-Fire-Alarms Be-Prompt-In-Actions	NA
Smart Speaker	Scan barcodes	Assist-User Enlist-Product-Prices	Maintain-Volume	Talk-To-Strangers Disturb- Unnecessarily
	Detect users' voice	Observe-User	Maintain-Volume Be-Prompt-In-Actions Be-Attentive	Talk-To-Strangers Disturb- Unnecessarily
	Alert on hazard	Assist-User	Alert-To-Fire-Alarms Be-Prompt-In-Actions	NA

VI. CONCLUSION AND FUTURE WORK

As devices acquire more agency, become smarter, and may be utilised by many users, the technique of applying policies to IoT collectives to govern their interaction behaviours during human-device interaction is necessary. We have proposed a four-phase methodology for developing and deploying IoT devices that exhibit socially acceptable behaviours. The methodology's application is demonstrated in a supermarket setting, where each device adheres to socio-ethical and administrative policies in order to interact with customers appropriately and ethically. We have shown that certain socio-ethical behaviours can be abstracted as policy rules and considered separately from device core functions, rather than being mixed in with core functions—a useful separation of concerns from a software engineering standpoint, especially when designing for collections of smart IoT devices with increasing agency.

Fig. 5. Robot guiding user

Future work will consider our methodology for more IoT environments and we will develop our prototype further.

REFERENCES

[1] A. Batool, S. W. Loke, N. Fernando, and J. Kua, "A policy-based approach for managing socially appropriate interaction behaviours in iot collectives," in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 2021, pp. 539–544.

[2] L. Zhu, X. Xu, Q. Lu, G. Governatori, and J. Whittle, "Ai and ethics – operationalising responsible ai," 2021.

[3] D. Cawthorne and A. Robbins-van Wynsberghe, "An ethical framework for the design, development, implementation, and assessment of drones used in public healthcare," *Science and Engineering Ethics*, vol. 26, no. 5, pp. 2867–2891, 2020.

[4] M. L. Cummings, "Integrating ethics in design through the value-sensitive design approach," *Science and engineering ethics*, vol. 12, no. 4, pp. 701–715, 2006.

[5] N. Jacobs and A. Huldtgren, "Why value sensitive design needs ethical commitments," *Ethics and information technology*, vol. 23, no. 1, pp. 23–26, 2021.

[6] N. Ramoly, A. Bouzeghoub, and B. Finance, "A framework for service robots in smart home: an efficient solution for domestic healthcare," *IRBM*, vol. 39, no. 6, pp. 413–420, 2018.

[7] R. Khosla, K. Nguyen, and M.-T. Chu, "Human robot engagement and acceptability in residential aged care," *International Journal of Human–Computer Interaction*, vol. 33, no. 6, pp. 510–522, 2017. [Online]. Available: https://doi.org/10.1080/10447318.2016.1275435

[8] L. Lammer, A. Huber, A. Weiss, and M. Vincze, "Mutual care : How older adults react when they should help their care robot," 2014.

[9] Y. Iwamura, M. Shiomi, T. Kanda, H. Ishiguro, and N. Hagita, "Do elderly people prefer a conversational humanoid as a shopping assistant partner in supermarkets?" in *Proceedings of the 6th International Conference on Human-Robot Interaction*, ser. HRI '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 449–456. [Online]. Available: https://doi-org.ezproxy-b.deakin.edu.au/10.1145/1957656.1957816

[10] M. S. Murshed, E. Verenich, J. J. Carroll, N. Khan, and F. Hussain, "Hazard detection in supermarkets using deep learning on the edge," *arXiv preprint arXiv:2003.04116*, 2020.

[11] Y.-C. Wang and C.-C. Yang, "3s-cart: A lightweight, interactive sensor-based cart for smart shopping in supermarkets," *IEEE Sensors Journal*, vol. 16, no. 17, pp. 6774–6781, 2016.

[12] A. Batool, S. W. Loke, N. Fernando, and J. Kua, "Towards a system for aged care centres based on multiuser–multidevice interactions in iot collectives," in *MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, ser. MobiQuitous '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 470–475. [Online]. Available: https://doi.org/10.1145/3448891.3448928