Operationalizing Rule-Based Socio-Ethical Behaviour in IoT Collectives: a Policy Management Approach

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

We are witnessing a trend of IoT devices with agency and often said to be smart (i.e., connected, sensor-equipped, and capable of autonomous action). This paper presents a policy management framework which we have named as the SANIJO policy framework. The framework consists of two types of policies, which are socio-ethical and administrative policies. Each policy further comprises three different types of rules, which are authorisation, obligation and prohibition rules that are applicable to smart internet-connected devices for managing their interactions in IoT collectives. An XML policy language which we have named as the SANIJO language is also designed for describing the desired interaction behaviours of smart devices. The policy management framework and the policy language are prototyped in the SANIJO system, which is a collection of mobile applications, multiple robot applications, smart speakers and smart camera applications. The SANIJO system is then illustrated based on an education open day scenario.

KEYWORDS

Education; Internet of Things; Interaction Behaviours; Policy Rules; Policy Management Framework

ACM Reference Format:

Amna Batool, Seng W. Loke, Niroshinie Fernando and Jonathan Kua. 2021. Operationalizing Rule-Based Socio-Ethical Behaviour in IoT Collectives: a Policy Management Approach. In *IEEE/WIC/ACM International Conference on Web Intelligence (WI-IAT '21), December 14–17, 2021, ESSENDON, VIC, Australia.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3486622.3493987

1 INTRODUCTION

Internet of Things (IoT) refers to the billions of physical devices around the world that are now connected to the Internet, all of which collect and share data. In this work, we have defined smart devices as *IoT collectives* which work together in a specific environment. Smart devices perform multiple actions and, while performing those actions, it is important to have control over their behaviour. There are numerous smart devices, particularly robots, that are used to create human-device interaction [13], [7], [8], but if a smart device interacts with multiple users, it is critical to know if the person next to it is comfortable interacting with such devices. To make the user next to a smart device comfortable, it is important to control the interaction behaviour of these devices.

A key premise of our work is that as Internet-connected devices get smarter, and become capable of autonomous action or are delegated tasks to perform, and they interact with users, their behaviours need to be managed in some way, and such devices need to behave within socio-ethical expectations of behaviour. For example, while assisting the users in an education center, the smart device must follow socio-ethical behaviours. Socio-ethical rules regulating smart behaviours can be identified and spelled-out explicitly in some language, and then either (i) applied at run-time to govern behaviours, and/or (ii) used as software engineering design artifacts capturing the socio-ethical aspects of smart device behaviours, in way that is separate from their core-functions.

We contend that socio-ethical behaviours can be abstracted as policy rules and should be considered separately from devices' core functions, instead of the consideration of such behaviours being mixed with core functions. To this end, this paper has the main contribution of proposing the SANIJO policy management framework and the SANIJO policy language to manage the interaction behaviours of smart internet-connected devices by imposing policies on them.

The rest of this paper is organised as follows. §2 presents the background and related work. §3 presents an overview of the SANIJO reference architecture and the framework, with respect to our education (campus open day) scenario - the framework comprises the set of policy rules and how they apply to different components in our architecture. §4 presents the SANIJO policies applicable to devices' core functions and their interpretation by the smart devices. §5 presents the SANIJO proof-of-concept prototype implementation and concept. §6 concludes with a discussion on future work.

2 BACKGROUND AND RELATED WORK

Smart internet-connected devices have different uses, but they have an open-ended dialog between the user and the smart devices, which is referred to human-device interaction [15]. During this interaction, it is important to investigate the interaction behaviours of smart devices to allow them to behave socially appropriately with the users. There has been considerable research conducted on human-device interaction, but restricted work has been done on interaction behaviours with a collections of smart devices [13], [7], [8].

Ricardo et al. [11] proposed a model-based security toolkit to enable the protection of user data in terms of security policies. There are certain policy rules (security and trust) specified in the

WI-IAT '21, December 14–17, 2021, ESSENDON, VIC, Australia

ACM ISBN 978-1-4503-9115-3/21/12…$15.00
https://doi.org/10.1145/3486622.3493987

toolkit using policy rule templates which follow an event-based ECA format. The toolkit also specifies a trust management rule template to build users' trust in IoT. The model has been prototyped and applied in smart city case studies to evaluate security policies. Unfortunately, the study has not focused on other aspects of IoT, such as handling uncertainties. Smart devices must be able to manage failures while performing any specific task, and our proposed framework contains multiple policy rules to handle uncertainty, secure user data, respect users' privacy, and so on.

Tj et al. [12] designed the HOMESNITCH framework for transparency and control of smart home IoT devices by identifying their semantic behaviour. The framework has been designed to use a random forest classifier to classify devices' behaviour and allow end users to control the smart home devices. Unfortunately, the HOMESNITCH framework can not identify the real-time behaviour of smart home devices. Moreover, the framework supports only smart home devices, whereas our SANIJO framework is applicable to multiple domains, including homes, supermarkets, aged care, and so on.

Faiza et al. [10] proposed a privacy-preserving IoT device management framework to enhance the privacy of smart devices. Data owners can predefined the privacy settings to allow the devices to perform actions based on those privacy settings. The devices can be controlled by smart contracts that can detect the misbehavior of each IoT device. The framework is very useful for enhancing the privacy of smart devices, but it is also essential to keep other behavioral aspects of smart devices.

Yefeng, Arjan and Lina [14] came up with a trust management framework designed based on measurement theory to allow users to measure the trustworthiness of smart devices. The study included various trust aspects among human-human and device-device trust relationships. The two metrics, i.e., trustworthiness and confidence, have been used to determine the trust relationships in IoT systems. The framework is useful for owners of different smart devices to measure the trustworthiness of their smart devices.

There are several uses of smart speakers around different domains, such as Alexa, Google home and many others. Some studies have conducted research on privacy perceptions of smart speakers. A research by Josephine et al. [9] investigated the privacy concerns of smart speakers by interviewing seventeen smart speaker users and seventeen non-users. Smart speaker users trust smart speaker companies that they will protect their privacy and non-users showed some concerns about privacy loss. The users were also unaware of privacy concerns. The authors recommended smart speaker companies to design the future smart speakers with incognito mode function and voice commands to mute the microphones to enhance the privacy of such devices. It clearly shows from this study that the privacy factor is important to consider in smart devices and our framework has socio-ethical obligation rules in which smart speakers, robots, smart cameras and other IoT devices respect the users' privacy, are transparent in their actions, follow the consensus seeking process and so on.

Marco et al. [4] focused on investigating the usage of smart speakers during Covid-19. The authors designed a questionnaire with 18 questions and asked the different users if they had bought the smart speakers during this pandemic situation. Most of the users answered "no", because of privacy concerns. Privacy is the main factor due to which most people do not buy such smart devices. Our SANIJO framework is designed with authorisation, obligation and prohibition rules which are applicable to multiple smart devices, including smart speakers. Smart speakers are authorised to assist users, but while assisting, they are obliged to seek approval before carrying out any action and are prohibited from responding to non-authorised (strangers) users.

Imposing socio-ethical policies on smart devices to allows them to respect users' privacy, keep them informed in each action, and many other such rules enhance the privacy of smart devices. It also builds users' trust in such devices and they try to interact with them easily. It is important for smart devices to make users comfortable while interacting with them. Therefore, our SANIJO framework comprises different policies through which the devices can interact with users conveniently. Moreover, it is not about a single smart device but the collections of IoT devices on which our proposed policies can be applied. Furthermore, the SANIJO framework is applicable to multiple environments, not just the educational domain. We have already investigated the applicability of our framework in an aged care scenario [1], but we plan to apply the framework to different environments too, such as agriculture, public spaces, supermarkets and many more. The video of our aged care scenario is at this link [1].

Our framework allows administration or owners of the environment to impose the administrative policies on the smart devices installed in their facility and the SANIJO language is designed to be processed by the smart devices to know how they will decode each policy applied to them.

3 OVERVIEW OF THE SANIJO REFERENCE ARCHITECTURE AND POLICY FRAMEWORK

3.1 SANIJO Reference Architecture

The SANIJO reference (abstract) architecture consists of a collection of IoT devices and mobile applications running on IoT devices, with three types of mobile applications: actuator applications that run on IoT devices, admin application that runs on the SANIJO administrator's device, and mediator applications that run on the smartphones of users. Users use the mediator applications to interact with devices controlled by actuator applications. The system administrator uses the admin application to set the policies for the devices. Figure 1 illustrates the components in the SANIJO reference architecture. There are multiple IoT devices that can run the actuator application, such as robots, smart cameras, smart speakers, and so on. Similarly, communicating as well as administrative devices can be smartphones, tablets, desktops, and so on, which can run mediator applications and administrator applications respectively. Each type of device performs different services. The IoT devices process policies and take requests from mediators (communicating devices) and mediators can send requests to actuators to allow them to perform different tasks. Administrators can use administrator devices to impose policies on actuators to control their interaction behaviour. IoT devices which run actuator applications process the

[1] See https://drive.google.com/file/d/1QpuOvoiRlhPYfY4oM_FZxE5muWmr5mRL/view?usp=sharing

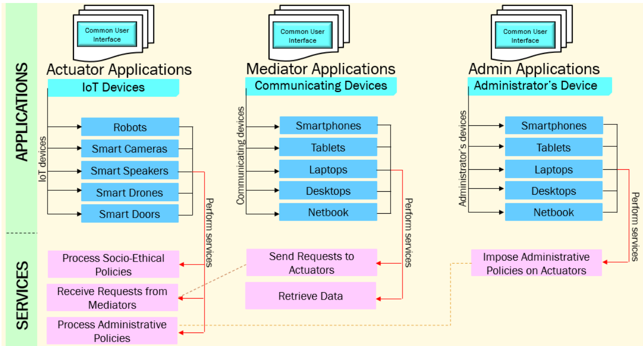

Figure 1: SANIJO Reference Architecture

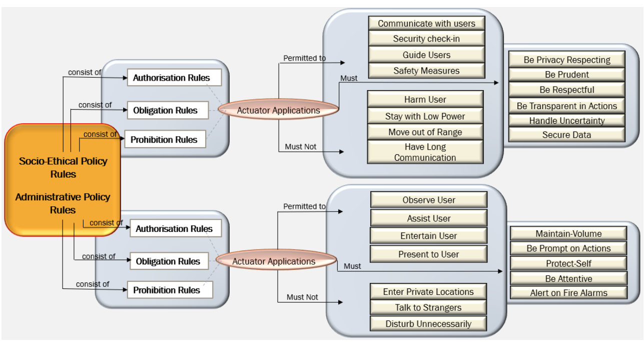

Figure 2: SANIJO Policy Framework: Education Domain

policies designed in the SANIJO framework, which are illustrated in detail in the next sub section.

3.2 Overview of the SANIJO Policy Framework

Figure 2 presents the SANIJO policy framework which consists of two types of policies, i.e., socio-ethical policy and administrative policy, which are applicable to actuator applications. Some of the examples of actuator applications in our work are smart robots, smart speakers and smart cameras. There are many more, but we have targeted these three devices in this work. Each policy (which we mean a set of rules) is outlined below:

- *Socio-Ethical Policy*, to control the socially appropriate interaction behaviours of smart devices.
- *Administrative Policy*, to govern devices with specific behaviours in specific environments.

Each policy mentioned above further comprises three different types of rules, which are authorisation, obligation and prohibition rules. The socio-ethical policy rules are pre-defined in the SANIJO policy framework, while the administrative policy rules need to be defined based on the environment in which the SANIJO framework applies. This is because the socio-ethical policy rules are designed to be applicable to all domains, including aged care centers, supermarkets, education centers, and so on. While the administrative policy rules need to be environment-specific. The socio-ethical policy applies in a variety of settings, but the administrative policy must be tailored to the circumstances. The rules in the socio-ethical policy are outlined below:

- *Authorisation Rules:* The authorisation rules are designed to manage the interactions and tasks which the device is allowed to perform. The authorisation rules designed are "communicate-with-users", "security-check-in", "guide-users" and "safety-measures".
- *Obligation Rules:* Smart devices must be obliged to follow some rules while interacting with different users. Therefore, the obligation rules are designed to manage the interaction behaviour of smart devices. The obligation rules designed are "be-respectful", "be-privacy-respecting", "be-prudent", "be-transparent-in-actions", "secure-user-data" and "handle-uncertainty".
- *Prohibition Rules:* It is essential to keep some limits on the actions that the devices can carry out. Therefore, prohibition rules are designed to enforce certain limits. The prohibition rules designed are "harm-users", "stay-with-low-power", "move-out-of-range of the permitted area" and "have-long-communication" - the device subject to this rule is prohibited from these.

As the administrative policy rules need to be defined based on the specific environment, this work has demonstrated the applicability of the SANIJO policy framework to an open day scenario at an education center. The administrative rules designed based on the educational environment are outlined below:

- *Authorisation Rules:* The authorisation rules under administrative policy are designed to control environment-specific tasks. Therefore, the authorisation rules defined based on education environment are "observe-user", "assist-user", "entertain-user" and "present-to-user".
- *Obligation Rules:* The obligation rules are designed to manage the environment-specific interaction behaviour of smart devices. Therefore, the obligation rules designed are "maintain-volume", "be-prompt-in-actions", "protect-self", "be-attentive" and "alert-to-fire-alarms".
- *Prohibition Rules:* It is essential to keep some environment-specific limits on the actions that the devices can carry out. Therefore, prohibition rules designed are "enter-private-locations", "talk-to-strangers", and "disturb-unnecessarily".

All of the rules mentioned above are intended to operationalize socio-ethical and administrative policies. The policies are further explained later in this work.

Each policy rule under a socio-ethical policy is designed based on ethical principles to operationalize ethical behaviour [3]. There are different ethical principles which have been linked with each socio-ethical policy rule to define the ethical interaction behaviour of smart devices in IoT collectives. The ethical principles targeted in our work are justice, beneficence, non-maleficence, respect for autonomy, fidelity, and confidentiality, taken from [5]. Figure 3 presents the ethical principles linked with socio-ethical policy rules. Each ethical principle is described in general but the examples are outlined from the education domain in an open day scenario.

- *Justice:* Justice is the principle of providing equal treatment, non-discrimination, and avoiding unfairness [3]. The justice principle is defined in our research as determining whether

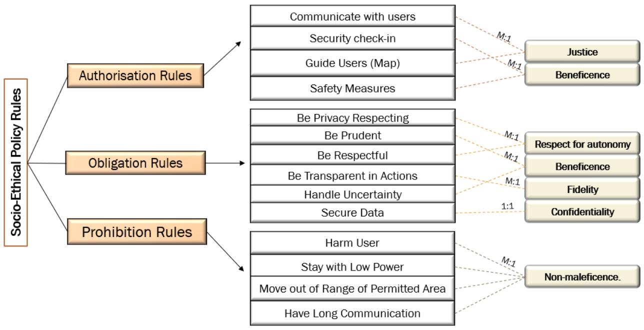

Figure 3: Ethical Principles linked with the Socio-Ethical Policy Rules

the behaviour of smart devices is fair and non-discriminatory towards users. Therefore, this principle is linked with authorisation rules, i.e., 'communicate-with-users' and 'guide-users'. For example, if a robot is communicating with students or staff on an open day at an institute, then the robot must be fair in communication with every student and staff.

- *Beneficence:* Beneficence is defined as doing good for others or benefiting the users [6]. This principle is determined in our research as whether the behaviour of smart devices benefits users. Therefore, this principle is linked with authorisation rules, i.e. 'security-check-in' and 'safety-measures' and the obligation rules, i.e. 'be-prudent' and 'handle-uncertainty'. In an education center on an open day, for example, if a robot is guiding a student to a library and encounters an obstacle, it alters the path to avoid the obstacle and guides users appropriately in terms of handling-uncertainty.
- *Non-Maleficence:* Non-Maleficence means do not cause pain to others [16]. In our research, non-maleficence determines if the devices' behaviour does not harm users. Hence, this principle is linked to all prohibition rules. For example, if a robot serves coffee to a staff member on an open day, then it is not permitted to go too close to the staff member, and this principle demonstrates that the devices' behaviour is not detrimental to society.
- *Respect for Autonomy:* Respect for Autonomy means one should be allowed to make decisions and choices [16], and in this work, this principle observes whether the behaviour of smart devices respects the privacy of users and allows users to make decisions. Thus, this principle is linked to obligation rules, i.e., 'be-prudent', 'be-privacy-respecting', and 'be-respectful'. For example, if a robot has to recognise a student's face, then it first takes approval from the student. If a student does not allow the robot to recognise his/her face, then the robot will not proceed.
- *Fidelity:* Fidelity is the principle of building trust between users and devices, or two parties involved in an activity [5]. In our research, Fidelity determines whether the behaviour of smart devices builds faith in society. Hence, this principle is linked with obligation rules, i.e., 'be-transparent-in-actions'. For example, if a robot is asked to take a student to the cafe, then the robot must inform the student about the location before moving, which shows that the student can have faith in a particular action performed by the robot following obligation rules.
- *Confidentiality:* Confidentiality manes not to disclose information [16]. To analyse if the devices' behaviour does not disclose users' data. In this work, this principle is linked with the obligation rule, i.e., 'secure-data'. For example, if a smart camera streams video of everyone moving around on an open day, then the smart camera must secure the streaming and must play in front of only the administration of an institute, which shows that the device is not disclosing the data to anyone else under the secure-data obligation rules.

4 POLICIES APPLICABLE TO DEVICES' CORE FUNCTIONS

The policies defined in the SANIJO framework are applicable to IoT collectives. Therefore, it is essential to mention the core functions of IoT collectives, including robots, smart cameras, and smart speakers, which our work targets, because each policy applies to actuators while they perform their core functions. Appendix A3 [2] summarises the core functions of each smart device and the preferred socio-ethical policy rules applicable to those core functions.

Throughout this paper, we illustrate our ideas via an open day scenario at an education center. Therefore, the administrative policy rules are designed to be applicable in the education domain. Appendix A5 [2] summarises the core functions of each smart device and the preferred administrative policy rules applicable to those core functions.

While performing the core functions, each actuator applies the policies mentioned in Appendix A3 and Appendix A5 [2], but once the policies are applied, the behaviour of smart devices will be changed. For instance, if a robot is interacting with users, it is not necessarily being very respectful to them, but after applying our proposed socio-ethical policy i.e., 'be-respectful', the robot will first greet the user and then interact with users.

Hence, the policy rules might imply behaviours additional to the core function or affecting the way the core function are performed.

SANIJO Language. Each policy rule is decoded differently by smart devices. Therefore, the SANIJO language is designed to let the devices learn what rules to follow and how to interpret each policy rule. For example, a robot is assisting a student by bringing him coffee on an open day and, at the same time, a smart camera is assisting a manager in streaming the event live. While delivering coffee, the robot encountered an obstacle, and the camera experienced a network outage. Both devices have to handle uncertainty, which means both devices have to carry out some action to deal with an issue in this case, but each will interpret this differently. The robot may change its path to avoid obstacles, while the camera will report the issue to the owner. In this way, the devices know how to decode each rule by processing the SANIJO documents, which contains operational interpretation of each policy for each type of device.

The SANIJO language comprises three different documents. One is about the policy rules to follow in each policy (socio-ethical and administrative policy), which are authorisation, obligation and prohibition rules. The second document is designed for the interpretation of each rule under socio-ethical policy and the last document is designed for the interpretation of each rule under administrative policy.

4.1 Devices' Behaviour After Socio-Ethical Policy is Applied

The socio-ethical policy reflects the ethics of smart devices to be followed while interacting with multiple users. Appendix A4 [2] outlined the interpretation of each rule under socio-ethical policy.

The full SANIJO language document on robot socio-ethical policy is available at this link [2]. Similarly, the complete document for the socio-ethical policy of smart cameras is available at this link [3] and the smart speaker socio-ethical policy document is available at this link [4].

4.2 Devices' Behaviour After Administrative Policy is Applied

The administrative policy rules are designed to be scenario specific. As, this research targeted the education environment to demonstrate the applicability of our framework. Therefore, the administrative policy rules are interpreted by actuators accordingly. Due to space limitations, here, we do not describe in detail the interpretation of the rules in the administrative policy. Appendix A5 [2] summarises the Administrative Policy rules and how they apply to core functions of devices.

The full document of the robot administrative policy is available.[5] Similarly, the complete document of the administrative policy for the smart camera is available,[6] and the smart speaker's administrative policy document is available.[7]

5 PROOF-OF-CONCEPT: THE SANIJO PROTOTYPE

With respect to the SANIJO reference architecture described earlier, SANIJO is a system implemented as a proof-of-concept and to demonstrate the applicability of our policies (socio-ethical and administrative) defined in the SANIJO policy framework and the SANIJO policy language on smart devices, explained in the last section. The concept and implementation of the prototype is explained within the context of use in an open day scenario in education. We consider an education scenario with deployed IoT devices, including multiple robots, smart cameras and smart connected speakers, as explained in the next sub-section.

[2]https://github.com/abatool-abatool/SANIJO-Language-Education-Domain/blob/main/Socio-Ethical-Policy-Robot
[3]https://github.com/abatool-abatool/SANIJO-Language-Education-Domain/blob/main/Socio-Ethical-Policy-Smart-Camera
[4]https://github.com/abatool-abatool/SANIJO-Language-Education-Domain/blob/main/Socio-Ethical-Policy-Smart-Speaker
[5]See https://github.com/abatool-abatool/SANIJO-Language-Education-Domain/blob/main/Administrative-Policy-Robot
[6]https://github.com/abatool-abatool/SANIJO-Language-Education-Domain/blob/main/Administrative-Policy-Smart-Camera
[7]https://github.com/abatool-abatool/SANIJO-Language-Education-Domain/blob/main/Administrative-Policy-Smart-Speaker

5.1 Targeted Devices and Mobile Applications

The Internet-connected Temi robots with software version 120.07 and launcher OS 1337, smart cameras and smart speakers OS Android, and multiple mobile devices OS Android are used to facilitate interactions between students, employees, administration, food stall people, and the devices themselves. All the devices can follow socio-ethical policies and imposed administrative policies while interacting with multiple users.

There are six different mobile applications implemented in the SANIJO prototype. The first is a robot application with all robotic features that can run on all Temi robots. The second application is for smart cameras and smart speakers with their perspective features. The third application is for the administration of educational centers who can use the app to impose administrative policies on smart devices (robots, smart cameras, and smart speakers). The fourth, fifth, and sixth applications are for students, staff members, and food stall people who can use their apps to send requests to robots, smart cameras, or smart speakers. Moreover, these users can also request these devices to assist, entertain, or present information to them. Appendix A1 [2] shows screenshots of the apps.

5.2 SANIJO Demonstration

In the SANIJO prototype, each actuator (i.e., robots, smart cameras, smart speakers) is assumed to be installed in an educational open day scenario where students, staff, admin and stall people can interact with these smart devices. Each device has to process the SANIJO language documents to know what rules they must follow and how to decode each rule while interacting with these users.

Figure 4 presents the whole scenario where the admin or manager uses his/her mobile app to impose administrative policy rules on all devices. After imposing the administrative policies, there are four Temi robots, one of them takes assisting requests from students and staff, e.g., to bring them food, coffee or fruits from three different stalls in terms of authorisation rules under the administrative policy. The robot takes the request and moves to the particular stall and asks the stall person to load the item. Once the stall person finishes loading the item, he/she selects "Thank You" shown on the robot's screen, then the robot moves back to the student or staff to offer them their requested item. While completing assisting requests, the robot adheres to administrative policies where it follows obligations as well as prohibition rules. This means robots will not enter into private locations, disturb users unnecessarily, or talk to strangers in terms of prohibition rules - even when requested (by users who are not the administrator). Moreover, the robot maintains volume, tries to carry out action as quickly as possible, protects itself from obstacles, and is attentive - as required by the imposed obligation rules under the administrative policy. Figure 5 shows a robot taking students' requests to bring them a food item (chocolate) from the stall and the robot moving to the stall and serving the item to the student (following administrative policy rules as it does so). In terms of socio-ethical policy, the second robot takes safety measures by moving to different stall locations and advises stall people to keep the floor clean at fixed time intervals, as shown in Appendix A2 [2]. Appendix A2 also shows the robot taking students' requests to guide them to the cafe. Also, stall people can use their mobile app to send a request to the smart speakers installed in

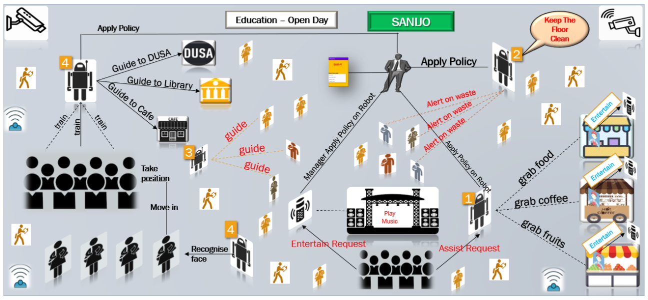

Figure 4: SANIJO Prototype Implementation in Education Domain

Figure 5: Robot moving to the stall (left), Robot bringing food item (chocolate) as per student request (right)

their stalls to play the music. The students can also send a request to smart speakers installed beside the stage to play the music for them. Similarly, the smart cameras are also assumed to be installed outside where they can observe the users by streaming and only admin can access the streaming through his/her mobile device.

6 CONCLUSION AND FUTURE WORK

The approach of applying policies on IoT collectives to manage their interaction behaviours during human-device interaction is required as devices are increasingly endowed with increasing agency and become smarter, and can be used by multiple users. We have proposed the SANIJO framework comprising two types of policies (socio-ethical and administrative) and the SANIJO language for interpretation of each policy by multiple smart devices. The applicability of the SANIJO framework and the SANIJO language is illustrated using an education environment (e.g., university) open day scenario where each device has followed the socio-ethical and administrative policies in order to behave suitably and ethically with users. We have demonstrated that socio-ethical behaviours can be abstracted as policy rules and can be considered separately from devices' core functions, instead of the socio-ethical considerations being mixed with core functions - a separation of concerns useful from a software engineering perspective, especially in view of designing for collections of smart IoT devices with increasing agency. Currently in Australia, Victoria, it is difficult to approach the organizations for user trial studies due to the tough COVID-19 restrictions but we have a plan to deploy our case study on education domains in the future.

ACKNOWLEDGMENTS

We acknowledge the support of Mr. Yousaff Nawaz from CASE University Islamabad, in this project.

REFERENCES

[1] Amna Batool, Seng W. Loke, Niroshinie Fernando, and Jonathan Kua. 2021. 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)*. 539–544. https://doi.org/10.1109/PerComWorkshops51409.2021.9431036

[2] Amna Batool, Seng W.Loke, Niroshinie Fernando, and Jonathan Kua. 2021. *Appendix Wi-IAT Paper* (2021). https://github.com/abatool-abatool/APPENDIX-WI-IAT-PAPER-2021/blob/main/Appendix___Wi_IAT_Paper.pdf

[3] Cansu Canca. 2020. Operationalizing AI Ethics Principles. *Commun. ACM* 63, 12 (Nov. 2020), 18–21. https://doi.org/10.1145/3430368

[4] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2020. On the usage of smart speakers during the covid-19 coronavirus lockdown. In *Proceedings of the 6th EAI International Conference on Smart Objects and Technologies for Social Good*. 187–192.

[5] Leslie Gelling. 1999. Ethical principles in healthcare research. *Nursing Standard* 13, 36 (1999), 39–42.

[6] Raanan Gillon. 1985. Beneficence: doing good for others. *British medical journal (Clinical research ed.)* 291, 6487 (1985), 44.

[7] Rajiv Khosla, Khanh Nguyen, and Mei-Tai Chu. 2017. Human Robot Engagement and Acceptability in Residential Aged Care. *International Journal of Human–Computer Interaction* 33, 6 (2017), 510–522. https://doi.org/10.1080/10447318.2016.1275435 arXiv:https://doi.org/10.1080/10447318.2016.1275435

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

[9] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.

[10] Faiza Loukil, Chirine Ghedira-Guegan, Khouloud Boukadi, Aïcha-Nabila Benharkat, and Elhadj Benkhelifa. 2021. Data Privacy Based on IoT Device Behavior Control Using Blockchain. *ACM Transactions on Internet Technology (TOIT)* 21, 1 (2021), 1–20.

[11] Ricardo Neisse, Gary Steri, Igor Nai Fovino, and Gianmarco Baldini. 2015. SecKit: A Model-based Security Toolkit for the Internet of Things. *Computers & Security* 54 (2015), 60–76. https://doi.org/10.1016/j.cose.2015.06.002 Secure Information Reuse and Integration & Availability, Reliability and Security 2014.

[12] TJ OConnor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. 2019. HomeSnitch: Behavior Transparency and Control for Smart Home IoT Devices. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 128–138. https://doi.org/10.1145/3317549.3323409

[13] Nathan Ramoly, Amel Bouzeghoub, and Béatrice Finance. 2018. A framework for service robots in smart home: an efficient solution for domestic healthcare. *IRBM* 39, 6 (2018), 413–420.

[14] Yefeng Ruan, Arjan Durresi, and Lina Alfantoukh. 2016. Trust Management Framework for Internet of Things. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*. 1013–1019. https://doi.org/10.1109/AINA.2016.136

[15] Eugenio Rubio-Drosdov, Daniel Díaz-Sánchez, Florina Almenárez, Patricia Arias-Cabarcos, and Andrés Marín. 2017. Seamless human-device interaction in the internet of things. *IEEE Transactions on Consumer Electronics* 63, 4 (2017), 490–498. https://doi.org/10.1109/TCE.2017.015076

[16] Basil Varkey. 2021. Principles of clinical ethics and their application to practice. *Medical Principles and Practice* 30, 1 (2021), 17–28.