The role of decisional autonomy in User-IoT systems interaction

Rino Falcone[1], Alessandro Sapienza[1]

[1] Institute of Cognitive Sciences and Technologies, National Research Council of Italy (ISTC-CNR), 00185 Rome, Italy

Abstract

As the Internet of Things (IoT) continues to spread, emerging technologies provide devices with various autonomous capabilities that enable them to assist their users in a multitude of activities throughout their daily lives. Despite this, it is still unclear what the role of autonomy should be in this context, as limited academic research has been conducted on such a topic. This study tries to fill this research gap, by proposing a possible solution on how IoT devices may act in order to develop and regulate their autonomy, in relation to the specific user they interface with. After introducing a theoretical framework, we considered a possible implementation in a simulation context, showing how the proposed approach works.

Keywords

Internet of Things, Autonomy, Trust, Social simulation, User acceptance

1. Introduction

In recent years, the concept of autonomy has played an increasingly important role in the context of the Internet of Things (IoT). As a matter of fact, IoT devices must be autonomous as well as cooperative in order to autonomously coordinate cooperative actions towards meeting common high-level goals [1]. Such autonomy allows them to improve their capability to sense, think, and act when executing tasks [2, 3].

Of course, the autonomy of the devices must always and in any case be confronted with the needs and availability of users. In this connection, Miranda and colleagues [4] introduced in their work the concept of Internet of People (IoP) claiming that, given the increasingly important role of technology in our daily lives, we as users should be put at the center of such systems. They stress the fact that IoT systems must be able to adapt to the user, taking people's context into account and avoiding user intervention as much as possible. In a similar way, Ashraf [5] talks about autonomy in the Internet of things, with the aim of arguing that in this context it is necessary to minimize user intervention. Nonetheless, research in this context is still scarce and the concept of autonomy has not yet been given all the attention it deserves [6]. There is still a gap in the literature regarding a comprehensive model that explains how IoT device should use and develop their autonomy in the relationship with the user.

WOA 2022: 23rd Workshop From Objects to Agents, September 1–2, Genova, Italy

*Corresponding author: Rino Falcone, rino.falcone@istc.cnr.it

rino.falcone@istc.cnr.it (R. Falcone); alessandro.sapienza@istc.cnr.it (A. Sapienza)

0000-0002-0300-458X (R. Falcone); 0000-0001-9360-779X (A. Sapienza)

Of course, there may be several approaches to address this problem. In this work, we focus our attention on a particular solution. Specifically, we take into account the fact that the devices possess a certain *autonomy of execution*, which determines the resources they need to perform in a certain way: internal/external resources, request for collaboration of other agents etc. In this sense, the more autonomous a device is, the less additional resources it needs to use. On the one hand, the performance of the devices is closely linked to this concept, so in some levels the devices can offer better results than others. On the other hand, the user may be more or less willing to grant the use of specific resources, thus desiring the execution of tasks at specific levels of autonomy.

Our idea is that devices can use their *autonomy of decision* as an opportunity to determine the best way to perform the task assigned to them, i.e. autonomously changing their level of execution. This ability requires various potentialities for our smart devices: i) to be able to manage its own different degrees of autonomy of execution in the interaction with the user; ii) to be able to evaluate and adapt, in each interaction, the right degree of autonomy of execution to carry out the task; iii) to know how to evaluate its own ability to act in the various degrees of autonomy of execution.

Therefore, within this article, we propose a framework analyzing the interaction between user and IoT device based on the concept of autonomy, in its different shapes. Specifically, we will investigate two different forms of autonomy: that of *execution*, which identifies what agents are able to do and what they are authorized to do; that of *decision*, or the degree of autonomy that agents have in determining their own autonomy of execution. By engaging in this exploration, this paper constitutes a step toward the study of the human-IoT systems interaction.

2. State of the art

While the fundamental role of autonomy has been clearly identified in the literature, there are few implementation solutions that have concretely given it a key role in the interaction with human users.

As a first example, in the HRI domain, the authors of Optimo [7] proposed a system capable of perceiving how much the user trusts the device and then adapting its behaviors dynamically, to actively seek greater trust and greater efficiency within future collaborations.

In the IoT domain, we introduced a model for user's acceptance [8], in which devices evaluated how much the user trusts them, in order to perform tasks with an adequate level of autonomy.

Hu and colleagues [9] conducted an experimental study to investigate the role of artificial autonomy by dividing it into three types of autonomy in terms of task primitives: sensing, thought, and action autonomy. In particular, the authors investigate how these dimensions affect the perception that users have of artificial devices (in terms of competence and motivation), in order to explain how these affect the willingness to use the devices themselves.

Recently, the authors of [1] introduced the concept of autonomy in large-scale IoT ecosystems, by making use of cognitive adaptive approaches.

Furthermore, Sifakis [10] states that IoT is a great opportunity to reinvigorate computing by focusing on autonomous system design. His idea is to compensate the lack of human intervention by introducing adaptive control.

Within this work, our efforts focus on determining how an IoT device can use and increase its autonomy of decision in the relationship with the user.

3. Model

In this work, we are interested in identifying the complex relations between a user u and an IoT system S consisting of n devices $\{d_1, d_2 \dots, d_n\}$. The human-device interaction model is based on the concept of autonomy. More specifically, we distinguish between 2 kinds of autonomy:

1. the *autonomy of execution*, *aut_e*, which defines both what devices are able to do and the resources to which they are authorized to access. This value is specified by the user when requesting the execution of a task;
2. the *autonomy of decision*, *aut_d*, namely the extent to which the devices can deviate from the level of autonomy of execution assigned by the user.

The devices represent the actors of this autonomy, while the delegators are the users. On the one hand, the user u makes use of the devices to perform the tasks it needs. At the beginning, the user u grants an initial level of autonomy of decision to the devices, defined as $predisposition$. Then, on each turn, the user will assign a specific task τ to a given device d_j, specifying also the level of autonomy of execution *aut_e* it desires. More in details, we classify the autonomy of execution in 5 levels:

- Level 0: to perform the task, in addition to the default internal and external resources, devices need another external agent and non-default external resources;
- Level 1: in addition to the default internal and external resources, devices need another external agent to perform the task;
- Level 2: to perform the task, in addition to the default internal and external resources, devices need to access other non-default external resources;
- Level 3: devices can execute the task with all internal and external resources by default. They cannot perform other tasks at the same time;
- Level 4: devices can perform the task with a minimum commitment of internal and external resources (by default) that is, you can be able to perform other tasks at the same time.

The idea is that the more autonomous the agent is in performing tasks, the fewer resources it needs. At the lowest levels, it needs to exploit external resources not directly available and/or other agents. Increasing the level, it no longer needs these resources. Indeed, at the highest level, it could even perform multiple tasks at the same time.

On the other hand, the devices want to satisfy at best the user's requests. However, in order to fulfill such purpose, it is sometimes necessary for the devices to modify their autonomy of execution [11, 12]. This shift in autonomy would give the device the chance to execute the task providing a greater performance.

At the end of the task, the performance of d_j is evaluated. The actual performance of the devices depends on the *error probability* of the considered task level.

3.1. The user

In the simulation, we considered a single user *u* dealing with a number of IoT devices. The user makes use of such devices to pursue its own goals, granting them an initial autonomy of execution, the *predisposition*, which limits their actions.

The *predisposition* takes into account the fact that different users may have different attitudes towards this type of technology. For instance, the authors of [13] found that household members with high technical skills are more willing to adopt smart home services and products.

Starting from this initial value, the autonomy granted may change over time in response to certain situations and may vary from device to device.

3.2. The devices

There can be a variable number of devices in the world. All of them possess the main goal of pursuing the user's task to satisfy at best its need (even those not explicitly requested). Remarkably, in order to do so, they need to increase their autonomy of decision *aut_d*.

The device may find itself in the situation of not being able to adequately perform a task at a given level of autonomy of execution, i.e. its expected performance is below a given threshold value σ. In order to overcome this issue, it can decide to change this level, by increasing or decreasing it.

Resuming, a device is characterized by:

1. Its *trustworthiness* estimation on the various levels, to evaluate its own skills in the different cases;
2. The autonomy of execution *aut_e*, assigned by the user;
3. The estimation of the autonomy of decision *aut_d*;
4. the *error probability* on each level: this is an intrinsic characteristic of the device, neither it nor the user can directly access it, but it can be estimated through interaction.

3.3. Trust and Autonomy

Trust is a key element in every aspect of social cooperation. Its importance has also been clearly recognized in Human-Machine interaction [14] and, more in details, also in the IoT domain [15]. In this paper, we refer to the socio-cognitive model of trust [16]. The trustworthiness [17] of the devices is modeled in terms of willingness and competence. As far as it concerns willingness, we assume in this case that the devices are always and in any case well disposed towards the user and that they have the main goal of satisfying its requests. Concerning competence, this dimension is implemented through the *errorprobability*, i.e. the probability that a device will not be able to successfully complete the requested task. Of course, this probability also depends on the level of autonomy at which the task takes place.

In the light of such premise, we have modeled the autonomy of decision as a scalar variable defined in [0,1], whereby the greater the autonomy the easier it is to switch level. Instead, the trustworthiness of a device is modeled as a 5 elements vector, precisely to evaluate its skill at every level of autonomy.

Of course, working at a given level of autonomy gives devices the opportunity to show their competence at that level. When a task ends, the trustworthiness is updated through a weighted mean, according to Equations 1. Here, $performance_{j,\tau,x}$ is the result of the execution of the task τ at level x by agent d_j, while γ_1 and γ_2 represent the weights of the old and the new value.

$$newTrustworthiness_{j,\tau,x} = \frac{trustworthiness_{j,\tau,x} * \gamma_1 + performance_{j,\tau,x} * \gamma_2}{\gamma_1 + \gamma_2} \tag{1}$$

Autonomy of decision is updated differently, according to 2.

$$newAut\_d_{j,u} = \frac{aut\_d_{j,u} * \gamma_1 + performance_{j,\tau,x} * \gamma_2}{\gamma_1 + \gamma_2} \tag{2}$$

Indeed, this should not increase if the device does not push beyond the level it normally performs. Therefore, the devices will detect those situations in which going further would represent an advantage for the user while not doing so would result in a loss and they will limit their increase of autonomy only to such situations. In this work we consider two condition to do so:

1. *base strategy*: the device believes that its performance at the assigned level will not be satisfactory (i.e., above a designated threshold σ);
2. *additional strategy*: besides the first strategy, the device will always try to modify the autonomy of execution, as long as there is sufficient autonomy of decision (above a designated θ threshold).

Once identified the need to change the level of execution, the device will choose an alternative level according to two factors: the probability *P_acceptance* that the user will accept the decision of the device and the gain G, in terms of performance, that would be obtained by choosing this new level. Equation 3 estimates $P\_acceptance_{u,j,\tau,x,y}$, i.e. the probability that the user u will accept the decision of the device d_j to increase the level from x to y, concerning the task τ. Such probability is estimated as a function of the *predisposition* of the user and the autonomy of decision *aut_d* of the device, developed through interaction with the user. The ϕ factor modulates the user's predisposition, shaping the fact that the more the device deviates from the assigned level, the easier it is for the task to be rejected.

$$P\_acceptance_{u,j,\tau,x,y} = (\frac{predisposition_u}{\phi} + aut\_d_{j,u}) * \alpha \tag{3}$$

$$\phi = \frac{\delta_{x,y}}{4} \tag{4}$$

Given the classification of the autonomy of execution, it is reasonable to assume that increasing the level is more convenient than decreasing it, as it requires fewer resources. Conversely, leveling down requires additional resources. To model this, we introduce the constant α in Equation 3. In the analogous case, when the level is decreased, α is replaced by β.

As far as it concerns the gain G, it is estimated as the difference between the expected performance (trustworthiness) at level y and the expected performance at level x, as in Equation 5.

$$G_{j,\tau,x,y} = trustworthiness_{j,\tau,y} - trustworthiness_{j,\tau,x} \quad (5)$$

We define probabilistic utility $PU_{u,j,\tau,x,y}$ as the product of $P\_acceptance_{u,j,\tau,x,y}$ and $G_{j,\tau,x,y}$ (see Equation 6. The device chooses the level with the greatest probabilistic utility. In case of equal result, the level with the highest G is preferred.

$$PU_{u,j,\tau,x,y} = P\_acceptance_{u,j,\tau,x,y} * G_{j,\tau,x,y} \quad (6)$$

4. Simulation and results

In this section, we present the results of the agent-based simulation experiments, implemented on the NetLogo platform [18]. In the simulations, we are going to check what happens in 3 different scenarios, namely:

1. *none*: there is no optimization mechanism;
2. *first*: only the base strategy is implemented, thus it is possible to modify the autonomy of execution if a low performance is expected (below the σ threshold);
3. *both*: the additional strategy is implemented, thus it is always possible to modify the autonomy of execution, as long as there is sufficient autonomy of decision (below the θ threshold).

The experiments were conducted using the following setting:

- *predisposition* = [0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1];
- *number of device*: 10;
- *duration*: 1000 time units;
- *error probability*: randomly assigned for each device on each level in the range [0,0.5];
- σ = 0.5;
- θ = 0.5;
- α = 1 and β = 0.9;
- γ_1 = 0.9 and γ_2 = 0.1.

Each run of the experiment has a fixed *duration* of 1000 time unit, enough time to stabilize the values of the variables of interest. Concerning *predisposition*, the whole range of values has been investigated. As for the *error probability*, it is randomly generated between 0 and 0.5. Such randomness is designed to ensure that each device must estimate its capabilities and evaluate on which levels it is appropriate to perform the tasks. The threshold σ has been set to 0.5, to ensure that devices provide an average performance greater than 50% when they decide to execute a task. In a similar way, the threshold θ ensure that, in the event that the device intends to optimize its performance even if its expected value is above σ, there is a certain probability of acceptance by the user. Then, α and β were set to shape the fact that it is more convenient to increase the level autonomy of execution that to decrease it. Lastly, γ_1 and γ_2 were set to give more importance to past experience and to avoid excessive fluctuations in the variable values during simulations.

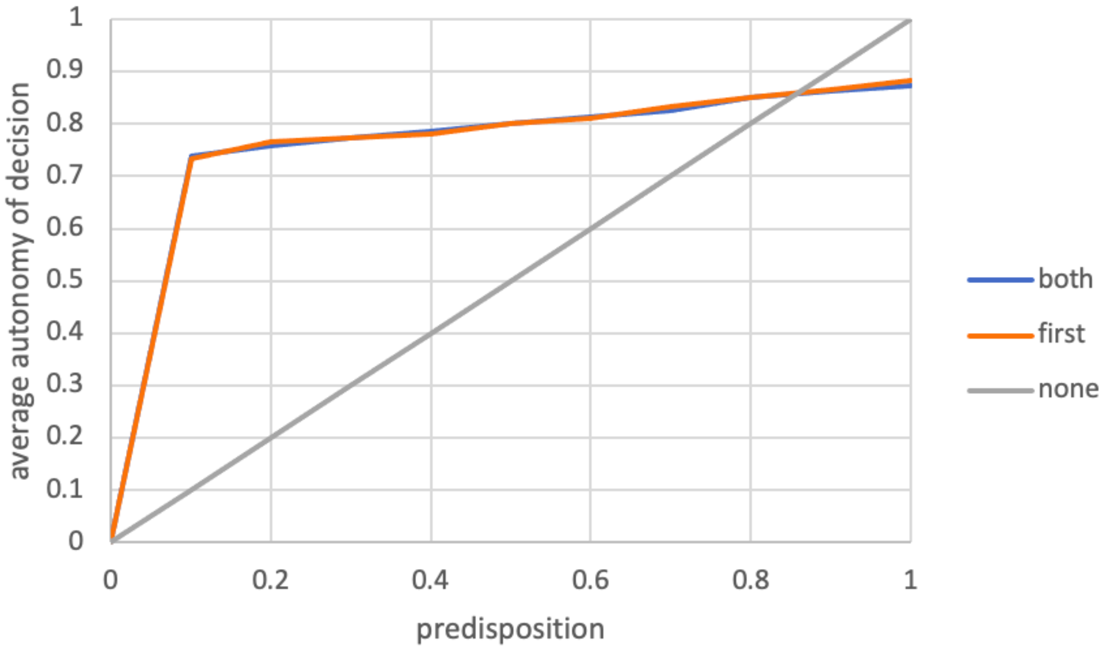

Figure 1: Evolution of average autonomy of decision, depending of the user's predisposition

Figure 1 shows the evolution of the autonomy of decision of the devices, as the user's predisposition varies. If neither of the two strategies is active, the autonomy granted remains exactly equal to the user predisposition. On the other hand, in the presence of one or two optimization mechanisms, the autonomy values increase significantly. We do not find significant differences between the two approaches, as far as it concerns autonomy of decision. In general, higher values of *predispositon* correspond to greater values of autonomy of decision. Such an increment is particularly significant in the proximity of the value 0, while immediately afterwards it remains linear. Basically, the more the user is willing to accept the autonomous choices of the devices, the easier it is for them to develop autonomy of decision: if the user rejects their choices, they have few possibilities for action. This result shows us how even a minimum predisposition value is enough to give devices the opportunity to develop their autonomy of decision.

Another remarkable result concerns the evaluation of trustworthiness, that is the perception that the user has of the devices. As Figure 2 shows us, the introduction of optimization mechanisms paradoxically involves a decrease in trustworthiness: in the considered level, -4.13% with the base strategy and -9.51% with the additional strategy. Although this effect may seem counterintuitive, the reasons for this result are clearly explained if we also take into consideration the variation of the performance provided to the user.

Thus, Figure 3 shows that the introduction of the base optimization strategy actually allows for an improvement on the performance provided to the user (+9.37% on average). Considering both strategies entails an additional increase (+13.52% on average). In fact, these optimization

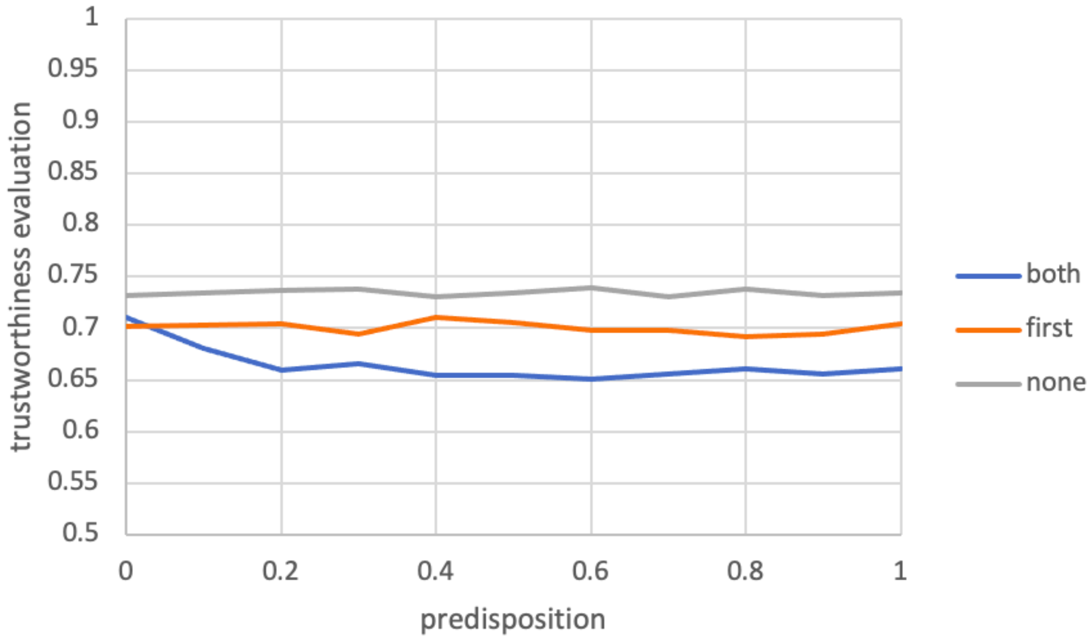

Figure 2: Evolution of average trustworthiness evaluation on level 4, depending of the user's predisposition

mechanisms ensure that devices operate on the levels at which they believe they are most efficient, avoiding those at which they are less good. As a consequence, the valuation for these low performance levels remains lower. This effect explains why the average trustworthiness evaluation decreases, as a result of the introduction of optimization strategies. However, this is in line with the main goal of the devices, as the main purpose of artificial systems should not be to maximize the user's perception of them [14]. While even this is an important topic, they should above all aim to improve the actual performance provided to the use, even if this involves being perceives as less trustworthy. It should also be noted that even in the absence of initial *predisposition*, the devices still manage to improve their performance.

5. Discussion and Conclusions

In this work, we investigated one of the possible approaches to increase autonomy of decision of IoT devices through direct interaction with a user.

Indeed, these devices have enormous potential to offer to end users. However, the user may not necessarily be willing to accept all the functionalities offered from the beginning. In light of such consideration, it becomes essential to understand how the device should behave in order to stimulate the user's trust and gradually ensure that the latter is willing to grant more autonomy. Of course, many approaches are possible to solve this problem [19, 20]. In this article, we have proposed a methodology in which devices exploit their autonomy of decision in order to offer better performance to the user, weighing the benefits introduced by deviating

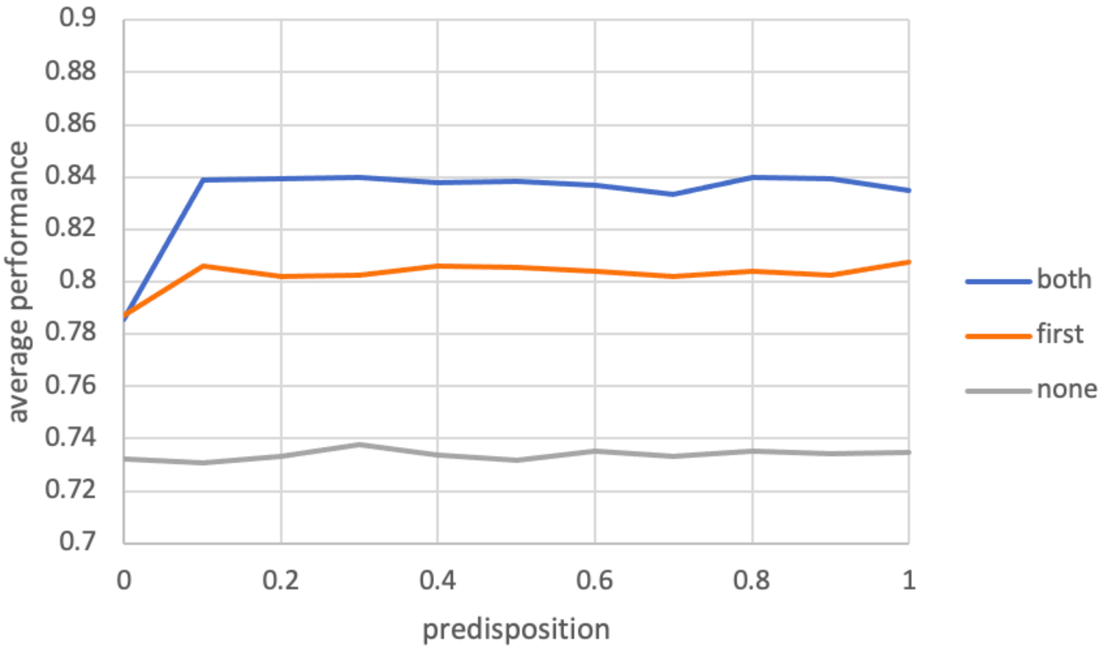

Figure 3: Evolution of average performance, depending of the user's predisposition

from what the user requests. This allows them to show their capabilities and, in turn, to obtain greater autonomy.

Summarizing the results of this analysis, we can say that:

1. Lower values of user *predispositon* correspond to lower values of autonomy of decision. Basically, the more the user is willing to accept the devices' autonomy of decision, the easier it is for them to develop such autonomy.
2. Allowing the devices to change the level of execution if they believe that their performance will not be satisfactory (*base strategy*) improves the performance provided to the user. Furthermore, allowing them to freely change the level of execution, as long as there is sufficient autonomy of decision (*additional strategy*) allows to get an even higher improvement.
3. Even in lack of *predisposition*, the optimization strategies allow to improve the performance.
4. Although these strategies improve the performance, the trustworthiness evaluation worsens, since the devices avoid performing task at some levels, in order to favor the levels at which they believe they perform better.

To conclude, the results of this work, albeit more theoretical, aimed at showing the effectiveness of the proposed approach, providing interesting insights for the evolution of IoT systems. Indeed, the experiments suggest that the approach used actually makes it possible to improve the levels of autonomy at which devices can operate.

It is worth underlining that the proposed framework is not intended as an alternative to the other solution to improve autonomy. On the contrary, it could provide support to other valid solutions.

References

[1] I. T. Michailidis, A. C. Kapoutsis, C. D. Korkas, P. T. Michailidis, K. A. Alexandridou, C. Ravanis, E. B. Kosmatopoulos, Embedding autonomy in large-scale iot ecosystems using cao and l4g-cao, Discover Internet of Things 1 (2021) 1–22.

[2] Y. K. Dwivedi, L. Hughes, E. Ismagilova, G. Aarts, C. Coombs, T. Crick, Y. Duan, R. Dwivedi, J. Edwards, A. Eirug, et al., Artificial intelligence (ai): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, International Journal of Information Management 57 (2021) 101994.

[3] K. M. Lee, J. Yoo, S.-W. Kim, J.-H. Lee, J. Hong, Autonomic machine learning platform, International Journal of Information Management 49 (2019) 491–501.

[4] J. Miranda, N. Mäkitalo, J. Garcia-Alonso, J. Berrocal, T. Mikkonen, C. Canal, J. M. Murillo, From the internet of things to the internet of people, IEEE Internet Computing 19 (2015) 40–47.

[5] Q. M. Ashraf, M. H. Habaebi, Introducing autonomy in internet of things, Recent Advances in Computer Science, WSEAS Publishing (2015) 215–221.

[6] E. Constantinides, M. Kahlert, S. A. de Vries, The relevance of technological autonomy in the acceptance of iot services in retail, in: 2nd International Conference on Internet of Things, Data and Cloud Computing, ICC 2017, 2017.

[7] A. Xu, G. Dudek, Optimo: Online probabilistic trust inference model for asymmetric human-robot collaborations, in: 2015 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI), IEEE, 2015, pp. 221–228.

[8] R. Falcone, A. Sapienza, On the users' acceptance of iot systems: A theoretical approach, Information 9 (2018) 53.

[9] Q. Hu, Y. Lu, Z. Pan, Y. Gong, Z. Yang, Can ai artifacts influence human cognition? the effects of artificial autonomy in intelligent personal assistants, International Journal of Information Management 56 (2021) 102250.

[10] J. Sifakis, System design in the era of iot—meeting the autonomy challenge, arXiv preprint arXiv:1806.09846 (2018).

[11] R. Falcone, C. Castelfranchi, The human in the loop of a delegated agent: The theory of adjustable social autonomy, IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 31 (2001) 406–418.

[12] R. Falcone, C. Castelfranchi, Levels of delegation and levels of adoption as the basis for adjustable autonomy, in: Congress of the Italian Association for Artificial Intelligence, Springer, 1999, pp. 273–284.

[13] J. Kowalski, C. Biele, K. Krzysztofek, Smart home technology as a creator of a super-empowered user, in: International Conference on Intelligent Human Systems Integration, Springer, 2019, pp. 175–180.

[14] A. Sapienza, F. Cantucci, R. Falcone, Modeling interaction in human–machine systems: A trust and trustworthiness approach, Automation 3 (2022) 242–257.

[15] G. Fortino, L. Fotia, F. Messina, D. Rosaci, G. M. Sarné, Grouping iot devices by trust and meritocracy, in: 2021 International Conference on Cyber-Physical Social Intelligence (ICCSI), IEEE, 2021, pp. 1–5.

[16] C. Castelfranchi, R. Falcone, Trust theory: A socio-cognitive and computational model, John Wiley & Sons, 2010.

[17] A. Sapienza, R. Falcone, Evaluating agents' trustworthiness within virtual societies in case of no direct experience, Cognitive Systems Research 64 (2020) 164–173.

[18] U. Wilensky, Netlogo. evanston, il: Center for connected learning and computer-based modeling, northwestern university, 1999.

[19] C. Kuhn, D. Lucke, Supporting the digital transformation: a low-threshold approach for manufacturing related higher education and employee training, Procedia CIRP 104 (2021) 647–652.

[20] C. Janiesch, M. Fischer, A. Winkelmann, V. Nentwich, Specifying autonomy in the internet of things: the autonomy model and notation, Information Systems and e-Business Management 17 (2019) 159–194.