How to Trust a Bot: An RPA User Perspective

Rehan Syed(✉) and Moe Thandar Wynn

Queensland University of Technology, Brisbane, Australia
{r.syed,m.wynn}@qut.edu.au

Abstract. Robotic Process Automation (RPA) has taken the industry by storm in recent years. Many organisations are keen to adopt RPA technology to dramatically improve their operational efficiency and digitally transform their business operations. However, industry reports and early academic research papers on RPA have highlighted various challenges associated with the use of RPA. Trust is one of the key factors that poses a challenge on the organisational acceptance of RPA. In this paper, we analysed the IS literature on trust to build an initial RPA-trust conceptual model. We then collected primary data from a selected group of RPA users to explore, explain, and confirm the factors that hinder building the user trust in bots using IT-artefact and Integrative model of organisational trust theories. The outcomes of this study are summarised in a conceptual model for RPA trust that will help organisations to build their strategies to effectively introduce and sustain RPA technology in their daily operations.

Keywords: Trust · Robotic Process Automation · IT-artefact · Qualitative case study · RPA-trust conceptual model

1 Introduction

In order to remain competitive and increase market share, organisations continuously seek out various opportunities to achieve service delivery excellence, cost efficiencies, profit maximisation and product innovation. Robotic Process Automation (RPA) is a recent automation technology that has created ripple effects in today's industry. Many organisations have been keen to adopt RPA technology to dramatically improve their operational efficiency.

RPA technology uses software to perform mundane and repetitive operational tasks by mimicking actions of a human user. This software (a.k.a. bots) can be used to follow a workflow with predefined steps, rule-based instructions and inbuilt functions to perform tasks such as copying data, sending emails, filling forms, going through verification and compliance checks, and updating different types of records. RPA has been termed as "macros on steroids" [23], as a bot can perform highly repetitive tasks with a high efficiency rate.

RPA is marketed as an ideal solution for organisations with labour-intensive processes that are high-volume and repetitive [1,17,22]. From an architectural

A. Asatiani et al. (Eds.): BPM Blockchain and RPA Forum 2020, LNBIP 393, pp. 147–160, 2020.
https://doi.org/10.1007/978-3-030-58779-6_10

perspective, RPA software does not integrate with an organisation's IT infrastructure; it works independently by using user-credentials to gain access to the required data and execute related software applications. This non-invasive nature of RPA results in a low turnaround time and less risks of unauthorised data access without the need for a major system or enterprise architecture modification. Not surprisingly, the promises made by RPA vendors managed to convince the industry to consider RPA technology as a serious contender for automation solutions.

A recent industry report mentioned a 30.14% RPA market growth rate that will lead to a $US 2.5 billion market size by the year 2022 [19]. A recent Forrester report [14] also confirms the high level of efficiency and improved customer services as key outcomes of RPA. Despite the high projection of success, RPA adoption is facing a number of challenges. Enterprise-wide stakeholder acceptance was mentioned as one of the key success factors for RPA [5,7]. Major consultancy firms also reported an estimated 50% failure rate, the inability to achieve the expected profitability targets, the lack of mastering RPA resilience, constant bot failures, and scalability problems [14].

User trust is one of the key challenges among many for RPA adoption [12] and plays an important role for organisational buy-in of RPA [4,23]. Automation carries a negative connotation from the users' perspective and is associated with resistance to change due to fear of job losses and redundancies.

With the introduction of RPA software, various human users and bots need to share the process and task responsibilities. More importantly, in line with Lee and See [18], the argument for increasing controlling roles of IT artefacts, bots are expected to take over a majority of mundane yet important process tasks previously performed by human users. As a bot takes over a significant amount of responsibilities from human users, the bot's performance is vital for the successful acceptance of RPA by users. It also requires a certain level of delegation between human users and bots to access the required corporate systems and data, and perform the assigned tasks. Hence, RPA must produce visible and tangible outcomes to build user trust [13]. We contend that the social acceptance of a bot as a "digital colleague" requires a deeper understanding of users' perspectives.

The insights gathered from recent RPA literature highlight the gaps in the viability of RPA technology to deliver the expected outcomes and raise concerns to investigate the notion of trust in RPA. We embarked on this study to understand "How trust is formed between human users and RPA technology?" We first analysed the IS literature on trust to build an initial RPA-trust conceptual model. We then collected primary data from a selected group of RPA users to explore factors that hinder building the user trust in bots. We positioned our findings using the IT-artefact and the Integrative model of organisational trust theories and proposed a conceptual model for RPA trust to assist organisations in developing strategies to effectively introduce and sustain RPA technology.

The rest of the paper is organised as follows. Section 2 provides a brief overview of trust in the Information Systems and RPA literature. Section 3

outlines the proposed two-staged constructivist grounded theory based research design. Section 4 presents our synthesis from user interviews whereas Sect. 5 provides a brief discussion. Section 6 concludes the paper.

2 A Brief Overview of Trust in Information Systems

The relationship between user trust and information system artefacts has been discussed extensively in past studies. The most common definition used by IS researchers for trust [18,28] is provided by Mayer et al. [20] which states that trust is the "willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that party" . Trust has been a key factor in major IS theories to analyse the behavioural intention and technology adoption and acceptance [24,32]. There are a number of studies measuring trust ranging from e-commerce, e-government, social media, to a variety of software systems [25,26].

Our search for literature related to RPA and trust was not able to find sufficient published research in this domain. RPA is a software artefact; therefore, we opted to extract the literature that explained the interrelationships between user trust and software/IT artefacts. In [9], the authors argued that trust in technology artefacts is equitable to inter-personal trust. The quality of the system, technical infrastructure, and the system's performance were identified as influencing factors for user trust [29].

A recent study on IoT and consumer acceptance [2] argued the importance of trust for IoT acceptance due to the novelty associated with the emerging domain. Along similar lines, understanding the effect of trust for RPA is required since it is an emerging technology and like any emerging trend, it suffers from limited user confidence in the promised technical capabilities as well as the socio-cultural aspects. A recent Forrester Consulting report [14] highlighted that the frequent bot failure is a key concern for the early adopters of RPA, hence the concerns with bot performance and reliability have a high potential to negatively influence user trust.

Most IS research on studying trust used Mayer et al.'s three dimensions of trustworthiness; namely, "ability, benevolence, and integrity" [20]. The **ability** dimension includes skills, competencies, and characteristics of a trustee (i.e., a bot) that enable it to influence a certain area of operations [20,28]. The **benevolence** dimension explains the perception of a trustee's intentions to bring genuine benefits to the trustor (i.e., a human user) beyond mere focus of financial and operational motives [20,28]. The **integrity** dimension explains the trustee's attitude towards adhering to certain principles that are important from the trustor's perspective. Furthermore, the vital impact of contextual factors (such as social influence, corporate policies, competitive pressure, etc.) on user trust has been extensively discussed in IS literature on technology adoption and acceptance [6,11,30]. Therefore, we opt to explore the contextual influences in the initial model to validate if there is any relationship between contextual influences and RPA user trust.

Figure 1 illustrates the initial framework developed as the synthesis of the trust factors identified in the literature.

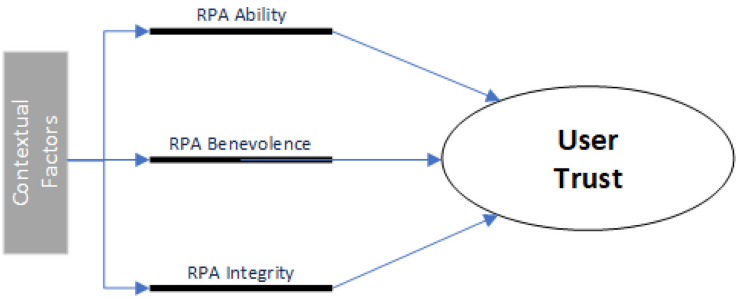

Fig. 1. An initial RPA-trust conceptual framework adapted from Mayer et al. [20].

3 Study Design

This study adopts a grounded theory approach [3,8,15,16] to explore the user trust factors for RPA. The constructivist grounded theory guidelines of [8] were used to design the research process. As suggested in [8], the constructivist design is useful to build theory by analysing systematically collected data using constant comparative analysis techniques. The constructivist grounded methodology is suitable to explore how social actors construct meaning in a selected domain of inquiry to build conceptual frameworks or theories using inductive analysis of qualitative data [8]. We collected data in two stages.

In stage one we performed a thorough literature review on IT trust and confidence factors by identifying 158 research articles available on Scopus. Each article was fully read and 33 articles with a focus on IT artefacts and user trust were extracted from the pool for deeper analysis. Selected articles were analysed using NVivo 12 as the data management software. The results of the literature review were used to define four dimensions for user trust in IT-artefacts and used to build an initial conceptual framework for user trust and RPA adoption.

In stage two we used a purposive sample to select our study participants. We invited selected staff from different organisations representing different industries, who have been using RPA for at least one year. The selected participants represented different roles and designations in their organisations; however, all participants closely engaged with the RPA software in their day-to-day operations. Five out of six interview participants belong to Banking, Financial Services, and Insurance (BFSI) domains in Australia and Sri Lanka. Each participant was actively engaged in RPA planning, design, and implementation activities in their organisations, whereas one participant was from an RPA consultant organisation.

Data was collected using semi-structured interviews. Six interviews were conducted with an average duration of 90 min. Each participant was requested to answer a set of open ended questions developed using the outcomes of stage one. Additional factors that did emerge from the primary data and not discussed in the literature were also accommodated. The details of the various dimensions of user trust and the areas for interview questions are provided in Table 1.

All primary data was then inductively analysed to explore the interrelationships and their dependencies. Data coding was performed in three iterations. In qualitative research, the coding is an analytical process to explore concept similarities, categorisation, and recurrence in data. In the first iteration, open coding was performed using the verbatim interview quotes. Coded data was compared and analysed to explore concept similarities. Next, focused coding was applied by labeling and re-grouping the coded data into suitable categories. The process was repeated after each interview to compare the coded data with the new data and categories were constantly redefined using inductive, deductive, and abductive reasoning [31]. The process continued until theoretical saturation was reached where no new categories emerged from the data. Next, theoretical coding was applied to synthesise and discover relationships and inter-dependencies between coded data. Theoretical coding is the process to explore and identify pattern and clues in analysed data [21]. Section 4 details the final deliberations and findings of the data analysis.

Table 1. Key dimensions of RPA-user trust.

Dimensions	Definitions	RPA trust construct
Abilities	This dimension includes skills, competencies, and characteristics of a trustee (i.e. the RPA Bot) that enables it to influence a particular area of operations [1, 2]	– Responsibility – Information Accuracy –Reliability
Benevolence	This dimension explains the perception of a trustee's intention to bring genuine benefits to the trustor (i.e. the end-user) beyond the mere focus of financial and operational motives (i.e. a mentoring relationship between a mentor (trustee) and a mentee (i.e. trustor) [1, 2]	– Authorised Data Usage – Designer Benevolence – User Understandability – Faith
Integrity	This dimension explains the trustee's attitude towards adhering to certain principles that are important from the trustor's perspective [1, 2]	– Predictability – Confidentiality – Data Integrity – User Authenticity
Context	The organisation factors that influence a trustor's perception of a trustee. The context may affect the other dimensions as a moderating factor	– Strategic needs – Policies – Associated risks

4 Findings

The following section provides a summary of the key themes that emerged from the interview data categorised into the four dimensions shown in Table 1. The findings are supported by selected interview quotes from different participants and evidences. The bold text refers to the main themes that emerged under each dimension of trust.

4.1 User Trust and Bot Ability

The **over expectation** relates to the users' perception on the bots' ability to perform an assigned task. It was mentioned as one of the main issues that influences user trust in RPA. The promises and hype created by the RPA vendors, market vibes, and organisational units responsible for implementing RPA solutions, as well as the management result in users developing high expectations of a bot's capabilities to perform the assigned tasks quite independently and with a high level of accuracy and reliability. However, as explained by the participant, when bots fail to perform due to several reasons, users get frustrated, they lose trust in the bots' capabilities. *"they thought it was going to be a lot more capable than it actually was so I think that people had very high expectations whether that came from the consultants or from their own imagination I don't know but they expected that the robot would know better"* (Participant 1); *"the concern is they will start the bot and they will lock their screen and go somewhere for a break, now bot is not able to recognise the screen elements, because system is locked, it will start showing errors, so according to them they are like the bot is not performing as expected"* (Participant 2).

Participants highlighted the vital role of the **consistency of data** and dependency of a bot on well defined data inputs. Inconsistent data sources severely hamper the bots' ability to process assigned tasks and result in users spending extra time and effort in cleaning up the data definitions. An oversight on effective data quality will result in users building negative perceptions and the loss of trust on the bots' ability. *"there was no discipline around it and I'll give an example of that is that the robot was checking names in the system to see whether it was already a customer and the people didn't adhered to a naming convention, so the robot would go in search for customer Jane Doe, but oh no, she's not there, people might have entered it as J Doe or Doe J or you know Doe Jane or whatever it might be and created a duplicate so then that's when trust again failed because they tried to implement something and there wasn't the discipline up front to set it up for success so that definitely was a problem"* (Participant 1). *"they haven't uploaded the file, bot was not able to extract the data and they were like no bot is not working today it's down, how do you process this many transactions? so it was the issue from their end"* (Participant 2); *"most of the issues were actually either the wrong process has been communicated to the bot or you know the whole hybrid coexistence issues where the bot is expecting a certain file or process to start from a particular location but that's missing, so we went through some of these issues"* (Participant 4).

Task visibility refers to the internal operations of a bot to process data. In a human-task environment, a user can comfortably send a request to another user to check the progress of an assigned task. However, a user expecting an output from a bot cannot view or query the status of a transaction. The 'black-box' nature of a bot, user curiosity and 'waiting' for an answer/output was explained as a contributing factor mentioned by the participants in building user trust. *"they lost visibility so they perceived the robot can do 8 things, so they would think you know, somethings gone into the bot and "I don't see it for 24 hours I*

don't know what's going on with it" so that kind of lack of visibility was definitely an issue. They were very much frustrated by that lack of visibility and I did not necessarily trust that what went in would be what came out" (Participant 2).

4.2 User Trust and Bot Benevolence

Design effectiveness refers to the bot designers' ability to accurately design and program a bot incorporating the users' key process requirements. The design effectiveness was explained as a critical issue since bots are personified and users literally blame the bot for a task failure even though the main issue lies with the programming and design of the bot. *"...they programmed it incorrectly, they personified the bot in a way that they were blaming the bot for getting things wrong. Now clearly it's not a bot that's got things wrong, its the programming of the bots by a human got it wrong in terms of not understanding the requirements*" (Participant 1). *"the performance of the bot depends on the developers who are building the bot, initially when they started building the bots, they were not using correct frameworks"* (Participant 2).

The interview participants strongly agreed that effective end-user engagement is crucial for building trust in bots. **End-user engagement** refers to the identification and involvement of key stakeholders during the design and productions stages of a bot. An oversight will result in an inefficient bot design and add to the users' frustration. *"if they had engaged the person [actual user] directly, she would have been able to give them a lot more information that would have made them be able to build the bot more effectively and would have preempted a lot of the problems, but they held back because I assumed that they thought she would be threatened by the bot"* (Participant 1).

Awareness of process complexity refers to the ability of RPA designers and business analysts to comprehend the scope, cross-functionality, steps involved in a process, and users' expectations from a particular bot. As mentioned by a participant, a key reason for lost user trust was related to the external consultants' inability to understand the context and complexities involved in a process. *"it was a more complex process then they thought and certainly initially the people who programmed it were external consultants and they were going by a standard that didn't apply in the context.... and so they wanted to impose a standard that just didn't work"* (Participant 1).

Another factor that emerged from the interviews relates to the technology support. **Technology support** refers to provision and availability of the required technical staff to provide hands-on assistance when a bot breaks down. *"we made sure that we got into details, vendor was literally you know on the floor throughout these three months, and hands-on, basically behind the persons' back, so something pops up, we addressed the issue then and there, so that's how we build user confidence and successfully transitioned"* (Participant 3).

4.3 User Trust and Bot Integrity

Data security refers to the users' trust in a bot's access to corporate data. The participants were from the BFSI industry that extensively comes under strict data security regulations and compliance requirements. However, these aspects of data security were not mentioned as an anxiety factor for user trust since a bot does not share their access credentials. *"from a security perspective, bots had their own logins so that there was no sharing in that respect, so that didn't become an issue"* (Participant 1). *"initially I was a bit concerned but then it was assured that bot can only access a team folder, it won't go beyond anywhere to just extract data from the portal, write it into the shared drive within a particular template. so yeah through this streamlined process the team was pretty much comfortable with that and now we're not facing issues like this"* (Participant 2).

Task delegation explains a user's perception towards sharing the assigned tasks with a bot. The participants were quite positive about sharing the workload with a bot, however, their main concern was about the availability of the required technical support to ensure task completion in case of a bot failure. *"I don't think they minded so much at the coalface, so I think that people who were receiving the output from the bot, their main concern was if the people [technical support] would be there for them"* (Participant 1).

4.4 User Trust and Contextual Influences

Fear of job loss was mentioned as one of the main factors that negatively associate with users' trust in bots. Not surprisingly, the participants unequivocally mentioned this factor as the main cause for resistance to change. The strategies to introduce automation and RPA are considered as ways to reduce cost by the management. *"I thought people will be threatened by it because that's what we have been told that it will take over jobs And all this kind of stuff"* (Participant 1).

Industry pressure refers to the organisations' response to industry-wide adoption of RPA to gain competitive advantage. The manner in which organisations pursue and introduce RPA in their operations varies from being a 'trend' follower to actually using the technology to genuinely develop their staff's job enrichment features. The participants explained this aspect as a driver for building staff's trust in corporate intentions for introducing RPA as a productivity tool rather than a cost minimisation tactic. *"I think there was almost like an industry pressure, certainly a senior who was the catalyst of the change was like 'well you know this competitor has done it, the big boys have done it, you know we should be doing it'. I think that was kind of potentially a driver or the desire to go in there plus I think it was a case of this is trendy we should be doing it"* (Participant 1).

Strategic direction refers to organisational focus on pursuing RPA as a robust strategy to improve staff capabilities and operational efficiency. The participants from the organisations where RPA faced stiff resistance to change and loss of user trust highlighted the absence of a cohesive and focused strategy as a result of senior management's lack of vision for RPA. *"a lot of the problems seem to be with the higher ups. Because there seemed to be a kind of almost like a turf war going on between senior levels, because you know they wanted to control the bot, they wanted it as their initiatives"* (Participant 1). On the other hand, the participants appreciated a well defined RPA strategy that created positive impression amongst the users. *"in our messaging we positioned RPA properly as an enhancement and industry first initiative which will give us a competitive edge, rather than we are going to replace you guys sort of thing"* (Participant 3).

The **top management support** was referred as a key driving factor to build user trust. Top management support involves the leadership from the senior management, and the provision of required resources for RPA adoption. The performance of RPA heavily depends on the technical infrastructure and the availability of technical support staff. Both aspects were mentioned as critical by the participants. Participants with a positive attitude towards RPA were quite appreciative of the level of technical support provided during the introduction stage. On the contrary, the absence of a good IT infrastructure and technical support worked negatively. *"they kind of brought together a kind of team, they weren't really IT but they were kind the robotics team, but they were understaffed, so the fact that they were understaffed again... they felt that they weren't able to support them well enough"* (Participant 1).

Data channel variations refers to the inconsistent document formats used by different sources that provide data for a bot. These variations tend to result in either process or business exceptions. The inflexibility of an associate organisation to align their reporting or document formats with a bot's process requirement can result in serious failures. Also, the bargaining power of an associate can determine the terms of engagement with a bot's processes. As mentioned by a participant, their organisation was in a high bargaining position and was able to demand their associates to sync their formats with the bots' required process. It is this variation that positively or negatively influences a bot's performance and affects the user trust. *"there were issues with the data formats... some of the payment channels [banks] were changing the way the files are, the templates that the statements are being delivered, so if the bot has been programmed to capture in one way and if the bank does the change, that will also impacting our day-to-day processes because then we have to retrain the bot to adjust to the new templates that being done at the payment channel level"* (Participant 4). *"if we are talking about volume, 20% of their volume came from branches and 80% came from brokers. The robot was only implemented for multiple reasons with the branches... and they couldn't even roll it out to the brokers because the brokers would have just said no I'll give you my form it's up to you to deal with it but there was also that level of trust and repeat business because brokers would give lots and lots of business. And if you mucked that up then they would just go to a different provider"* (Participant 1).

Awareness of RPA capabilities refers to the users' understanding of the links between the complexities associated with process executions and RPA capabilities. This lack of understanding creats higher expectations amongst RPA users. In general, users tend to believe that a bot has intelligent capabilities and is able to work quite independently even though their organisation uses an attended bot that requires users' intervention to complete an assigned task. *"they lack the understanding in technical terms, what a bot can access what a bot can't access. so that is the issue and since it is a very new term for almost all the organisations right now they don't know that deep understanding how this whole automation works behind the scenes"* (Participant 2).

5 Discussion

In this section, we provide a brief discussion on the factors identified and the interrelationships between different aspects. In general, the factors explained in Sect. 4 are quite close to the general causes for any standard software application. However, the key differences lie with the manner in which organisations approach RPA technology adoption. The participants with a high degree of trust acknowledged that a robust change management strategy is vital to build user trust in RPA. The training of a bot as well as the users was mentioned as the winning strategy. The quality assurance and testing of a bot's performance was key to build user trust. During the production phase, the target should be on achieving a high level of performance validation with an 85 to 100% bot accuracy. The bot designers' technical skill levels and comprehension of an end-to-end process can directly effect the users' trust in a bot.

As explained by a participant, *"Initially some of the teething issues were mainly related to training, on two sides you see the bot had to be properly trained. Because like with any other business case, the initial requirement gathering you may not gather 100% of the requirement on day one...then we had to train obviously the same set of users. We can't be parallel running with the bot since the bot is obviously faster so we narrowed down those number of users, I think we ended up with only one or two users maximum and we got them to shadow the bot until the errors were zeroed and as of today, the number of errors are zero and the number of human errors also are zero"* (Participant 3).

The lack of awareness and knowledge of RPA and its capabilities was another important factor that must be considered before deployment of a bot. The business teams without having a deep understanding of their processes and contexts in which a process is performed, and associated complexities will produce insufficient or incomplete requirements needed for a bot developer. The processes to automate belongs to the operations team in most organisations. The operations team must develop their technical understanding and the internal details of how a whole process works and integrates with a bot to overcome performance issues. As mentioned by a participant, a well defined process is the key for an effective bot design which will in turn be able to perform as per the user's expectations. *"we took around two months time to develop the process, it was very difficult,*

so many applications, national applications were involved, we delivered that as well. Even though that bot was only producing around 70% accuracy of the task, but still they were very happy because we have reduced their time, so I think this is the thing, mutual understanding between the team, when they start understanding the capability of the bot and start trusting it after the first use of their product" (Participant 2). The findings reflect that the human personification of bots (i.e., creating a human identity for a bot) without creating proper awareness can also result in negative consequences and confusions (see, Sect. 4.1 - Over expectations and Sect. 4.2 - Design effectiveness). The personification created a false assumption amongst human users that a bot is equivalent to humans in terms of its capabilities and its ability to make critical decisions.

The issue of user trust is also attributed to the development of attended bots where the coexistence between human users and a bot was required due to the nature of the process. Interestingly, the implementation teams did not come across user trust issues and in fact mentioned their own confidence on the abilities, and integrity of a bot. *"For compliance it was much smoother because there was no human interventions. Yes, there is no human intervention, it is the bot runs as scheduled"* (Participant 5). A bot will perform the way it is designed to perform, therefore, the notion of trust actually depends on the manner in which the requirements are identified by the business analyst/operations team, the accurate identification of required inputs, the data format, training of the bot to reach a comfortable level of accuracy, and the users' training and awareness.

6 Conclusions and Future Research

Advances in digital technologies also introduce new challenges regarding their adoption within an organisation. For organisations keen to adopt RPA technology, the social acceptance by human users of a RPA bot as a "digital colleague" is crucial to ensure smooth and seamless operations. Current literature on RPA demonstrates that user trust is one of the key challenges of RPA adoption.

This paper proposes a conceptual model for the RPA-trust framework, which is built on the three dimensions of trustworthiness, namely "ability, benevolence and integrity" [20]. Primary data from interviews with six RPA experts is then used to analyse key factors that hinder building users' trust in bots using the IT-artefact and the Integrative model of organisational trust theories. The first set of interview findings shows that organisations embarking on their RPA journey should pay attention to building a mutual understanding between the operations teams and RPA designers; ensuring relevant stakeholders are identified and closely engaged with; building the confidence of human users by providing much needed technical support; and implementing an effective change management plan. Furthermore, the deployment of a bot to handle actual tasks must only be performed after a rigorous quality assurance and performance assessment. Our findings also point out that most of issues can be addressed by existing knowledge (see [10]) related to software design, testing and implementation.

This study has several limitations. The data was collected from a small number of respondents from similar industries and therefore, lacks the generalisability of key findings. The interview participants were from technical backgrounds and provided their views from a technical perspective. In future, we aim to alleviate these limitations by following a mixed method approach. In line with Shenton [27], the credibility will be achieved by interviewing additional participants from different domains to increase the richness and variety of data. For triangulation, a Delphi study approach will be pursued to get the 'expert' consensus on findings. In addition, the findings will be confirmed by using a quantitative survey approach with a large sample size.

References

1. Aguirre, S., Rodriguez, A.: Automation of a business process using robotic process automation (RPA): a case study. In: Figueroa-García, J.C., López-Santana, E.R., Villa-Ramírez, J.L., Ferro-Escobar, R. (eds.) WEA 2017. CCIS, vol. 742, pp. 65–71. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66963-2_7
2. Aldossari, M.Q., Sidorova, A.: Consumer acceptance of internet of things (IoT): smart home context. J. Comput. Inf. Syst., 1–11 (2018)
3. Barney, G., Anselm, S.: The Discovery of Grounded Theory, pp. 1–19. Weidenfield & Nicolson, London (1967)
4. Bawack, R.E., Samuel, F.W., Kevin, C.: Artificial intelligence in practice: implications for is research. In: 25th Americas' Conference on Information Systems (AMCIS), pp. 1–10. Association of Information Systems (2019)
5. Beers, A., Heijndijk, R., van Dalen, C.: Understanding the challenge of implementing your virtual workforce: Robotic Process Automation as part of a new social-technological paradigm (2018). https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/strategy/deloitte-nl-so-understanding-challange-of-implementing-rpa.pdf
6. Bunker, D., Kautz, K., Anhtuan, A.: An exploration of information systems adoption: tools and skills as cultural artefacts-the case of a management information system. J. Inf. Technol. **23**(2), 71–78 (2008)
7. Carden, L., Maldonado, T., Brace, C., Myers, M.: Robotics process automation at techserv: an implementation case study. J. Inf. Technol. Teach. Cases **9**(2), 72–79 (2019). https://doi.org/10.1177/2043886919870545
8. Charmaz, K.: Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. Sage, London (2006)
9. David, G., Paul, P., Izak, B., Harrison, M., Katherine, S., Detmar, S.: ICIS panel summary: should institutional trust matter in information systems research? Commun. Assoc. Inf. Syst. **17**(1), 9 (2006)
10. Davis, F.D., Venkatesh, V.: Toward preprototype user acceptance testing of new information systems: implications for software project management. IEEE Trans. Eng. Manage. **51**(1), 31–46 (2004)
11. Dayan, M., Di Benedetto, C.A.: The impact of structural and contextual factors on trust formation in product development teams. Ind. Mark. Manage. **39**(4), 691–703 (2010). https://doi.org/10.1016/j.indmarman.2010.01.001

12. Dintrans, P., Anand, A., Ponnuveetil, M., Dash, S., Ray, K.: How digital 2.0 is driving banking's next wave of change (2017). https://www.cognizant.com/whitepapers/how-digital-2-0-is-driving-banking-s-next-wave-of-change-codex2865.pdf
13. Dunlap, R., Lacity, M.: Resolving tussles in service automation deployments: service automation at Blue Cross Blue Shield North Carolina (BCBSNC). J. Inf. Technol. Teach. Cases **7**(1), 29–34 (2017)
14. Forrester Research: Barriers and best practices for scaling RPA: centralized automation, resiliency, and low-maintenance bots pave the way to RPA success. Technical report, Forrester Consulting (2020)
15. Glaser, B.G.: Advances in the Methodology of Grounded Theory: Theoretical Sensitivity. Sociology Press, Mill Valley (1978)
16. Kathy, M., Linda, J., Josselson, R., Anderson, R., McSpadden, E.: A constructivist grounded theory analysis of losing and regaining a valued self. In: Five Ways of Doing Qualitative Analysis. Phenomenological Psychology, Grounded Theory, Discourse Analysis, Narrative Research, and Intuitive Inquiry, pp. 165–204. The Guilford Press, New York (2011)
17. Lacity, M., Willcocks, L.: Robotic process automation at Telefonica O2. MIS Q. Execut. **15**(1), 21–35 (2016)
18. Lee, J.D., See, K.A.: Trust in automation: designing for appropriate reliance. Hum. Factors **46**(1), 50–80 (2004). https://doi.org/10.1518/hfes.46.1.50_30392. PMID: 15151155
19. Markets, Markets: RPA market global forecast to 2022, markets and markets, March 2017 (2017). https://www.marketsandmarkets.com/Market-Reports/robotic-process-automation-market-238229646.html?
20. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Acad. Manage. Rev. **20**(3), 709–734 (1995). http://www.jstor.org/stable/258792
21. Melanie, B., Jane, M.: Grounded Theory: A Practical Guide. Sage, Los Angeles (2015)
22. Mendling, J., Decker, G., Hull, R., Reijers, H.A., Weber, I.: How do machine learning, robotic process automation, and blockchains affect the human factor in business process management? Commun. Assoc. Inf. Syst. **43**(1), 19 (2018)
23. Mitra, S.: RPA's adoption challenges & how to solve them (2019). https://it.toolbox.com/guest-article/rpas-adoption-challenges-how-to-solve-them
24. Oliveira, T., Martins, M.F.: Literature review of information technology adoption models at firm level. Electron. J. Inf. Syst. Eval. **14**(1), 110 (2011)
25. Pang, M.S., Lee, G., DeLone, W.H.: It resources, organizational capabilities, and value creation in public-sector organizations: a public-value management perspective. J. Inf. Technol. **29**(3), 187–205 (2014). https://doi.org/10.1057/jit.2014.2
26. Qin, L.: A cross-cultural study of interpersonal trust in social commerce. J. Comput. Inf. Syst. **60**(1), 26–33 (2020)
27. Shenton, A.K.: Strategies for ensuring trustworthiness in qualitative research projects. Educ. Inf. **22**(2), 63–75 (2004)
28. Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., Leimeister, J.M.: Understanding the formation of trust. In: David, K., et al. (eds.) Socio-Technical Design of Ubiquitous Computing Systems, pp. 39–58. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05044-7_3
29. Vance, A., Elie-Dit-Cosaque, C., Straub, D.W.: Examining trust in information technology artifacts: the effects of system quality and culture. J. Manage. Inf. Syst. **24**(4), 73–100 (2008)

30. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**(3), 425–478 (2003). http://www.jstor.org/stable/30036540
31. Ward, K., Gott, M., Hoare, K.: Analysis in Grounded Theory-How Is It Done? Examples From a Study That Explored Living With Treatment for Sleep Apnea. SAGE Publications Ltd., London (2017)
32. Li, X., Valacich, J.S., Hess, T.J.: Predicting user trust in information systems: a comparison of competing trust models. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences, p. 10 (2004)