Human Interaction and Emerging Technologies (IHIET 2022), Vol. 68, 2022, 605–611
https://doi.org/10.54941/ahfe1002783

Designing Trustworthy IoT Systems: Critical Challenges and Approaches for Generating Value

Boyeun Lee, Adrian Gradinar, Rachel Cooper, and Paul Coulton

Lancaster Institute of Contemporary Art, Lancaster University, Bailrigg, Lancaster LA1 4ZA, UK

ABSTRACT

At the end of the 20th century, the Internet of Things term was first introduced. Since then, the phenomenon behind this technological development is still fast-growing with estimates of more than 24 billion IoT devices readily connected to the Internet by 2030. During use, each of these devices generates valuable data for the end-user whilst negotiating the cybersecurity challenges low secured IoT devices employ. Whilst these security challenges have presented businesses with extensive opportunities for value creation, there are only a handful of studies exploring the challenges and opportunities related to security, privacy, and trust in IoT platforms and systems from a business perspective. Through a series of semi-structured interviews with top-level managers of different organisations across various industries in the UK, a methodological approach was developed to capture and address IoT value creation from the business' perspective in which trust factors are at the core of the value creation process. This research identifies four critical challenges and approaches to value creation namely: continuous scaling-up, co-creation, data-driven value creation, and user-centric design. These approaches provide a comprehensive understanding of how value creation activities are critically related to cyber security and how they affect trust factors. This study contributes to initiating the body of literature regards cybersecurity and business application. It also enables industry practitioners to generate value from IoT whilst better understanding the relations between value creation activities and cybersecurity concerns.

Keywords: Value creation for IoT, IoT trust, Design challenges, Design strategies

INTRODUCTION

The term Internet of Things (IoT) was firstly coined by Kevin Ashton in 1999 to illustrate how everyday things could make use of data they gathered, short of human intervention, to "observe, identify and understand the world – without the limitations of human-entered data" (Ashton, 2009). What originally started as a catchphrase for a presentation (Elder, 2019) is, two decades later, a global phenomenon, where even mundane objects, such as a Nespresso machine (Ziegler, 2016) or a pair of flip flops (Warren, 2017) are connected to the Internet. Statista (2022) forecasts a triple increase of IoT devices from 7.74 billion in 2019 to 25.44 billion by 2030. Equally, the total global market for IoT technologies is predicted to generate anywhere from

$2.7 trillion to $14.4 trillion in value by 2025 (McKinsey, 2013). Crucially, it is broadly understood that the mixture of physical and digital components brings great opportunities for innovation and value creation in businesses (Nasiri et al., 2017; Yoo, 2013).

Compared to traditional products, value creation from IoT is critically distinctive: the connectivity, real-time data, and embedded software enable the scope, features, and value of digital offerings to continue evolving, long after the product's launch day. The value propositions could be delivered with a combination of multiple products and applications through an integrated holistic platform. IoT as a new source of 'big' data helps businesses enter new relationships with their customers (Rymaszewska et al., 2017) and continuously reshape business models and strategies (Porter & Heppelmann, 2014). Whilst real-time data, embedded software, and connectivity enable continuous value creation for businesses, it also brings new cybersecurity challenges, such as data anonymity, confidentiality, and integrity (Sicari et al., 2015); system vulnerability; security and privacy; trust and trustworthiness (Pan & Yang, 2018). This research is concerned with the last challenge mentioned, namely building a trustworthy IoT system.

Trust and Trustworthiness in IoT systems

In the context of digitalisation, the broad and complex conception of trust can be understood as "building a computing system that provides reliable services to its end users while maintaining their data privacy and application security" (Jararweh et al., 2020). In informational technology services including IoT, several technical concerns can negatively affect the building of a trustworthy system. The scalability of the IoT system stemming from the interconnected and distributed computing systems amplifies the trust concerns (Voas et al., 2018). Intangible communications between different devices, processing, and handling of data to comply with user needs and rights. Data ownership and transparency emanate from users' perceptions of uneven distribution of benefits of the IoT services being skewed in favour of input suppliers (Voas et al., 2018). Therefore, trust has a more pivotal role in the success of IoT business (Khan et al., 2016) because it is interrelated to guaranteeing system security, user safety, and adoption (Gefen et al., 2003). Although trust and trustworthiness in IoT systems are critical issues in businesses' value creation (Mashal et al., 2015), there are only a handful of studies conducted addressing the IoT trust concerns from the business perspective (Lu et al., 2018). In response to the above-identified challenges, in this study, we explore the existing IoT trust model introduced by AlHogail (2018), and identify four critical challenges and opportunities in creating value and building trustworthy IoT systems.

METHODOLOGY

In this study, six informants from healthcare, smart home, drain maintenance, dairy, vertical farming, and tropical farming participated in semi-structured interview for data collection. Through deductive analysis, using AlHogail's factors as predefined themes (2018), sixteen challenges and approaches for IoT development and value creation were identified. They were then grouped

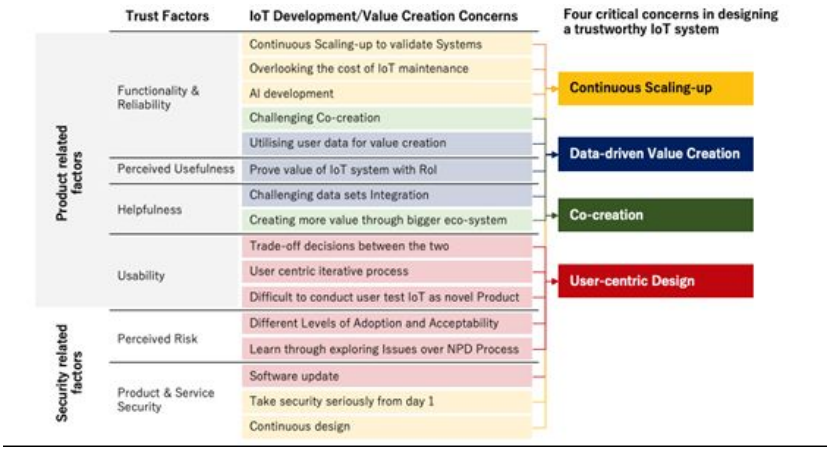

Figure 1: Four critical challenges and approaches to creating value of and designing a trustworthy IoT system.

into the four critical challenges and approaches to designing a trustworthy IoT system (See Figure 2) which are discussed in the following section.

FINDINGS AND DISCUSSION

Continuous Scaling Up

Scaling up is required for various reasons, for example, the IoT system application to different circumstances and settings, integration of a company's IoT system with others, replacement of the physical components, or release of updated software patches, which are representative of a critical issue relevant to the trustworthiness of the IoT system. Voas et al. (2018) identify scalability as one of the concerns that negatively affects trustworthiness of IoT system. For instance, the drain maintenance company's founder believes scaling up is useful to enhance the accuracy of system by obtaining more data and validating algorithms.

The system working perfectly for any circumstances, contexts and settings is crucial to enhance system reliability and trust (Voas et al., 2018). The interviewee of the smarthome IoT describes that they had to go through the review process every twelve months to ensure their products are appropriately designed. As IoT businesses scale-up, the range of the target customers becomes broader, and it may require the system amendment for adoption. Integrating one IoT system with others could be another critical challenge. This heterogeneity creates emergent behaviours that enable new and unforeseen security vulnerabilities while also affecting other issues related to reliability and performance (Voas et al., 2018). For example, the drain maintenance IoT company had to continuously provide customers support, including software updates, and solving technical faults whilst integrating the IoT system to the customers' system. One of the overlooked developmental concerns is the cost of IoT maintenance. Data reliability and availability is crucial in building customers' trust (Voas et al., 2018) which may increase businesses storage and maintenance costs. More significantly, the vertical

farming IoT and the drain maintenance company, did not know if their device would last 20 years and therefore could not estimate the maintenance cost. They believe that data availability affects customers' adoption of the system further impacting the organisation's long-term commitment to the IoT system.

A dramatically accelerating pace in digital technology development affects the continuous design led to security vulnerabilities. Due to the fast speed of digital technology advancement, the components used to develop the IoT system became quickly outdated or no longer available which often meant replacing the component. One replacement of a component may result in the whole system being redesigned or the whole software being updated because of new security vulnerabilities that could be discovered. As indicated during the interview with the leader of the healthcare IoT project, the detection of a security vulnerability in a chip may require the change to the software, which may also require the hardware's change. Equally, the smarthome IoT recognised the data security is significant, further hindering its addition to the IoT system once its architecture was developed. Thus, they were cautious about data management and put a significant amount of effort, cost, and expertise from the beginning. For example, after designing the IoT system securely, they hired penetration testers to hack the system and audit the code. To ensure privacy, they accessed customers' data, only in the presence of the customer and the data was kept encrypted at the CCTV so that only customers have the key to decrypt their own data.

User Centric Design

User-centric design is a pivotal factor in the development of trustworthy IoT systems and is related to trust factors such as usability, perceived risk, and product and service security. For example, a software update is inevitable as a possible solution to preventing the security issue. However, the difficulties of updating software for IoT should be understood as it is often a constrained device (Voas et al., 2018). The co-founder of the smarthome IoT explained that if an IoT system is designed to have high security, it would possibly be not user-friendly designed. Accessibility or, ease of use of a technology, plays a pivotal role in building user trust (Gao & Bai, 2014; Lai et al., 2011) which is observed in the development case of tropical farming IoT and drain maintenance IoT. The target market of the tropical farming IoT is the farming industry in tropical regions, such as East Africa and Central America, where farmers rarely have access to smartphones. Thus, the tropical farming IoT had to develop different methods of providing information to the farmers, such as SMS and voicemail, which were already available. Similarly, the drain maintenance company raised critical questions related to user-centric design, such as the type of devices and the data format.

One of the noteworthy obstacles in user-centric design is to obtain enough user insight. The project leader of the healthcare IoT explained that having user feedback was impossible unless the system was fully developed. In the feasibility testing stages, their value constellation (Normann & Ramírez, 1994) was incomplete and consequently, the user feedback ought to be

limited. Alternatively, the co-founder of the tropical farming IoT described that it was difficult to obtain sufficient insights into how the users interact with the system and receive feedback on the UI and UX of their products and services. Unfortunately, the users were not able to use the system which is unsurprising given that IoT is an entirely new technology, bridging both the physical and digital words. Therefore, leveraging existing technological user-centric models is challenging.

Data-Driven Value Creation

Data is understood as a noteworthy business asset by the interviewees. The companies collect data on the customers, environment, and devices, which keeps their value propositions evolving to enhance the user experience. For example, in the dairy IoT case, while the feature of fertility monitoring was being provided to the farmers, monitoring health solution, identified from the data and market feedback, was added to the existing system. Companies also create value through aggregating diverse datasets but when the IoT system has large ecosystem, trust concerns might be multiplied (Palattella et al., 2016; Voas et al., 2018). Building trust in data-driven value with customers is significant for IoT businesses. Providing a clear value proposition affects conventional practitioners' adoption of digital tools (Hale Group, 2014). In the dairy IoT case, the farmers whose practice is entrenched do not tend to trust the system unless the Return on Investment (RoI) of the system is proved. Helpfulness is one of the crucial trust factors as data sets integration may provide users with appropriate, effective, and timely advice that may be required to complete a task. However, if the quality of the data is not satisfied, it will directly impact trustworthiness of IoT system (Voas et al., 2018). The interviewee of the drain maintenance company argued they spent extra time ensuring the accuracy of the data their systems provide. The founder of the dairy IoT business described they have different types of digital data available but without data standards there are too many challenges related to the cross-integration of datasets to generate value.

Value Co-Creation

Value co-creation is stressed as a core approach for complex IoT development across companies. However, it also generates new types of security and privacy threats (Feltus & Proper, 2017). All interviewees explicitly or implicitly describe that they have implemented co-creation to create more value for their businesses. Helpfulness of the IoT system, one of the trust factors, could be increased when more devices are interconnected, and more data are shared. IoT companies could build their own unique eco-system while partnering with other companies. However, the leader of the healthcare IoT business explained that it may make the system more vulnerable since data being shared with co-creators may result in higher data breaches. Vicini et al. (2016) argue that big data shared by a number of stakeholders in distributed environment is one of the challenges of co-creation. Moreover, the managing director of the drain maintenance company stated that each stakeholder has different interests and security issues. It is burdensome for

them to build a holistic platform through which stakeholders' products and applications interoperate.

CONCLUSION

This paper provides a comprehensive understanding of how value creation activities and trust issues mutually interact and influence each other. The study has identified four challenges and approaches in designing trustworthy IoT systems from the business perspective: continuous scaling up, user-centric design, data driven value creation, and value co-creation. Continuous scaling-up is inevitable to increase data accuracy, availability, and reliability but it may also bring trust concerns, including unexpected behaviours, technical errors, and data breach. User centric design is compulsory despite a tension between security and usability. However, several hindrances are observed against user-centred design such as different level of adoption and acceptability, a constrained interface of IoT device which deliver the right amount and types of real-time data further hindering obtaining user feedback. Data driven value creation and co-creation are a part of the fundamental IoT business activities, but they may increase trust threats. Some of the concerns are interrelated to each other, for instance, having data shared within value constellation is related to co-creation, continuous scaling up, and data-driven value creation. Whilst this study produced clear benefits for the business sector, it also contributes to the academic body of literature regarding cybersecurity and business applications. Finally, this research will enable industry practitioners to understand the relations between value creation activities and cybersecurity concerns from managerial perspectives.

ACKNOWLEDGMENT

The authors would like to acknowledge the contributions offered by participants within this research study. The research presented in this paper has been possible through the PETRAS IoTHub, funded by the UK Engineering and Physical Sciences Research Council (EPSRC), and Research and Development Management Association (RADMA) Doctoral Funding.

REFERENCES

AlHogail, A. (2018). Improving IoT Technology Adoption through Improving Consumer Trust. *Technologies*, *6*(3), 64.

Ashton, K. (2009). That "Internet of Things" Thing. *RFID Journal*. Retrieved from http://www.rfidjournal.com/article/print/4986

Doney, P. M., Barry, J. M., & Abratt, R. (2007). Trust determinants and outcomes in global B2B services. *European Journal of Marketing*, *41*(9/10), 1096–1116. https://doi.org/10.1108/03090560710773363

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and tam in online shopping: AN integrated model. *MIS Quarterly: Management Information Systems*, *27*(1), 51–90. https://doi.org/10.2307/30036519

Hale Group. (2014). *The digital transformation of row crop agriculture, Iowa AgState Big Data Project Report*.

Jararweh, Y., Otoum, S., & Ridhawi, I. (2020). Trustworthy and sustainable smart city services at the edge.pdf. *Sustainable Cities and Society*, *62*, 1–11.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2016). Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model. In J. Park, H. Jin, Y. Jeong, & M. Khan (Eds.), *Advanced Multimedia and Ubiquitous Engineering* (pp. 111–117). Springer.

Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of Things_ A systematic review of the business literature from the user and organisational perspectives | Elsevier Enhanced Reader. *Technological Forecasting & Social Change*, *136*, 285–297.

Mashal, I., Alsaryrah, O., Chung, T., Yang, C., Kuo, W., & Agrawal, D. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, 68–90.

McKinsey. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. *McKinsey*. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/disruptive-technologies#

Nasiri, M., Tura, N., & Ojanen, V. (2017). Developing Disruptive Innovations for Sustainability: A Review on Impact of Internet of Things (IOT). In *Proceedings of PICMET '17: Technology Management for Interconnected World*.

Normann, R., & Ramírez, R. (1994). *Designing Interactive Strategy: From Value Chain to Value Constellation*. Chichester ; New York: John Wiley & Sons, Inc.

Pan, J., & Yang, Z. (2018). Cybersecurity challenges and opportunities in the new "edge computing + iot" world. In *SDN-NFVSec 2018 -Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization* (pp. 29–32). Association for Computing Machinery, Inc. https://doi.org/10.1145/3180465.3180470

Porter, M., & Heppelmann, J. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*. Retrieved from https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

Radziwon, A., Bilberg, A., Bogers, M., & Madsen, E. S. (2014). The smart factory: Exploring adaptive and flexible manufacturing solutions. In *Procedia Engineering* (Vol. 69, pp. 1184–1190). Elsevier Ltd. https://doi.org/10.1016/j.proeng.2014.03.108

Rymaszewska, A., Helo, P., & Gunasekaran, A. (2017). IoT powered servitization of manufacturing–an exploratory case study. *International Journal of Production Economics*, *192*, 92–105.

Sicari, S., Rizzardi, A., Grieco, L., & Goen-Porisini, A. (2015). Security, Privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

Voas, J., Kuhn, R., Laplante, P., & Applebaum, S. (2018). *Internet of Things (IoT) Trust Concerns*. Gaithersburg, Maryland. Retrieved from https://csrc.nist.gov/publications.

Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics and Computer-Integrated Manufacturing*, *28*(1), 75–86. https://doi.org/10.1016/j.rcim.2011.07.002

Yoo, Y. (2013). The Tables Have Turned: How Can the Information Systems Field Contribute to Technology and Innovation Management Research? *Journal of the Association for Information Systems*, *14*, 227–236.

Ziegler, C. (2016) Why does this Nespresso machine have Bluetooth? https://www.theverge.com/2016/2/23/11099500/nespresso-prodigio-bluetooth-coffee-machine