Overcoming Cloud Concerns with Trusted Execution Environments? Exploring the Organizational Perception of a Novel Security Technology in Regulated Swiss Companies

Tim Geppert
ZHAW Zurich University of Applied Sciences
Winterthur, Switzerland
Tim.Geppert@zhaw.ch

Jan Anderegg
ZHAW Zurich University of Applied Sciences
Winterthur, Switzerland
Anderja3@students.zhaw.ch

Leoncio Frei
ZHAW Zurich University of Applied Sciences
Winterthur, Switzerland
freileo1@students.zhaw.ch

Simon Moeller
ZHAW Zurich University of Applied Sciences
Winterthur, Switzerland
moellsim@students.zhaw.ch

Stefan Deml
dq technologies AG
Zurich, Switzerland
stefan.deml@decentriq.ch

David Sturzenegger
dq technologies AG
Zurich, Switzerland
david.sturzenegger@decentriq.ch

Nico Ebert
ZHAW Zurich University of Applied Sciences
Winterthur, Switzerland
Nico.Ebert@zhaw.ch

Abstract

Trusted execution environments are a new approach for isolating data, specific parts of code, or an entire application within untrusted cloud environments. This emerging security technology could also enable the migration to cloud infrastructures for organizations working with highly sensitive data. As current research does not address the organizational perception of trusted execution environments (TEEs), we conducted an explorative study to clarify the technological, environmental, and organizational views on this technology by health care, life sciences, and banking companies in Switzerland. The interview findings show that in these industries, missing technological knowledge as well as privacy and process regulation are perceived to be the most critical driver for organizational adoption of TEEs. The identified low intrinsic motivation to adopt novel technologies permits us to conclude that clarifying the regulatory impact of TEEs could drive future adoption by organizations.

1. Introduction

As cloud computing systems and services are complex in nature and enable a multitude of technologies that can be deployed in different ways, achieving a sufficient understanding of how to secure such systems is a significant challenge [9]. Furthermore, cloud computing users lose control of the data as they do not manage the physical infrastructure on which their data is stored [14]. The need for privacy-friendly solutions is especially prevalent in regulated sectors like banking, life sciences, and the health care businesses, where privacy risks for sensitive data are a significant drawback of cloud systems [10]. More specifically, potential threats include data leakage of sensitive medical records, which can, in turn, lead to patients being discriminated against by employers or health care insurance agencies [8]. However, due to the low cost, high efficiency, scalability, and availability, highly regulated companies are now moving to cloud systems [9], and TEEs are being introduced to enhance the security of these systems [6]. Thus, the technology could potentially provide the necessary security guarantees to facilitate cloud adoption within regulated industries. Although there is a broad body of knowledge covering the organizational adoption of cloud computing, to our knowledge, there is currently no study of the influencing factors for the corporate adoption of TEEs in regulated industries. As companies working with sensitive data will benefit most from additional security measures, our study focuses on these specific industries. Consequently, the research question in our study aims to explore factors perceived to affect the organizational adoption of TEEs within the Swiss health

URI: https://hdl.handle.net/10125/80164
978-0-9981331-5-7

care, life sciences, and banking sectors. As the current literature does not give sufficient insight regarding this issue, we conducted semi-structured interviews based on the technology organization environment (TOE) framework [25]. The TOE has been applied to analyze the adoption of various technical innovations in organizations [19, 21, 27] in the past. This study seeks to close the research gap on adoption factors for TEEs. These factors can potentially have a transforming impact on security-related barriers to the adoption of cloud computing.

2. Trusted Execution Environments

The three pillars of data security involve protecting data at rest, in transit, and in use. Conventional cloud computing infrastructure struggles to protect data in use (e.g., cloud providers cannot prove to the customer that they have not accessed their data). However, TEEs enable the secure execution of code within cloud environments. Security is provided by encrypted memory regions called enclaves [6]. Predefined algorithms can be sealed within the TEE and used to calculate insights on provided data. Furthermore, the output format and aggregation level of the resulting data can be predefined, and output is only provided for defined users. Hardware-based TEEs within cloud environments are termed "confidential computing" by various vendors such as AMD, Intel, and ARM, and on different platforms such as Microsoft Azure or IoT applications [22].

Figure 1 gives a high-level overview of the principal stages of creating and using a TEE based on Intel SGX. The system's author must create the TEE, a so-called enclave [6]. During this development phase, hardware-specific security keys are used to seal the parts of the application that need additional security guarantees (Figure 1a). A user wanting to work with an enclave can first obtain proof of the software and hardware via an attestation service provided by Intel (Figure 1b). This proof is based on the sealed security keys and information about the software, which can be accessed by the user and sent to the attestation service. Following successful attestation, the user can provide his or her data to the enclave to be processed and receive an output.

3. Research Approach

Literature Review. A literature review following recommendations by Webster & Watson [28] was conducted in November 2020. The scope of this literature review was to identify existing studies providing an organizational lens on trusted execution environments. We used the keywords "trusted execution environment" and one of the following second terms: "business perspective," "organization," or "TOE." Searches were done in the following databases: Web of Science, ProQuest, and Google Scholar to cover a broad range of journals [29]. We could not find any relevant literature that provided an organizational perspective on TEEs within the databases based on these keywords. Using the keyword "TEE" alone revealed several publications that all focus on the general conceptualizations of the technology [11, 12, 13] and on the technological feasibility perspective [26], where performance is presented as the primary technical drawback [2]. In addition, the research focuses on the isolation, encryption, and attestation schemes of TEEs [16, 17, 18, 20].

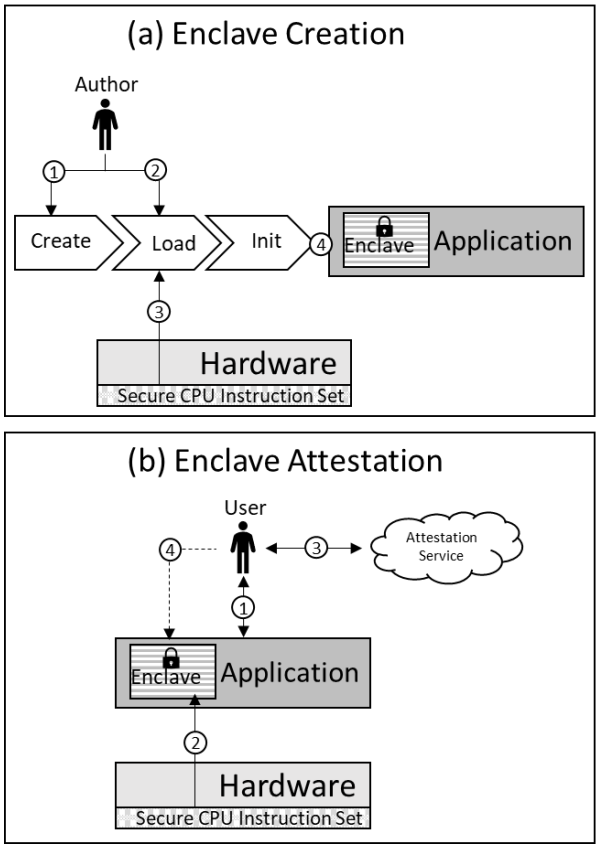

Figure 1*:* The enclave creation and attestation process.

Interview Method. We conducted explorative interviews with business stakeholders from regulated industries to fill the research gap regarding the organizational perception of trusted execution environments. In these interviews, we used the terms TEE and confidential computing synonymously, as practitioners typically use the latter. The experts were

selected from three different regulated industries, working with personally identifiable data and with diverse backgrounds and roles [4]. We deliberately concentrated on IT professionals with security and managerial expertise since relevant experts of a novel technology are not easy to identify. Our chosen specialists could simultaneously understand the innovative potential of the technology and provide information about the business impact of such technology within their organization and industry. The interview guide followed the methodology of Bogner et al. [4]. We provided key questions and follow-up questions within the semi-structured interviews based on the individual answers and TOE lenses. This approach was chosen as the technology is new, and we wanted to add further insights to the existing body of knowledge. In addition, we were interested in the perception of this technology from the three viewpoints of the TOE framework as described by Tornatzky & Fleischer [25], so we structured the questions with these in mind. The leading questions in the interviews were deductively structured as follows. First, we posed questions about the challenges that could be solved with innovative security technology in the respective industry to find common ground regarding technology innovation. Then we followed up with questions concerning the anticipated benefits of confidential computing projects and the significant barriers of such projects in the respective industry, based on the TOE lenses. The results are presented according to these lenses.

Interview Evaluation. A total of 13 interview participants were interviewed by video in spring 2021. Interview times ranged between 26 and 58 minutes, with 40 minutes on average, resulting in a total of 9.5 hours. All but two of the interviews were transcribed. Participant P2 [L] and P3 [L] declined to be recorded because of confidentiality concerns. However, written notes were taken during these two interviews. Next, one of the authors deductively coded each interview, the coding categories being based on the TOE lenses. After this, a second author analyzed the codes across the boundaries of the individual interviews. Finally, the coding results were discussed among the researchers to remove bias and strengthen their validity.

4. Findings

Interviews were conducted with 13 interview participants who are key stakeholders in relevant IT areas within their respective companies, as shown in Table 1. Five interviewees were from the life sciences sector, four from the health care sector, three from the banking sector, and one works for a cloud provider.

Table 1: Overview of the interview participant sample. Key: Life sciences [L], health care [H], banking [B], and cloud provider [C]

Participants	Job Description/Title
P1 [L]	IT Security Officer
P2 [L]	Head of IT Operations
P3 [L]	SAP and HR IT Services Manager
P4 [L]	Chief Information Officer
P5 [L]	IT Risk Security Manager
P6 [H]	Head of IT Operations
P7 [H]	Head of IT
P8 [H]	Head of IT Infrastructure
P9 [H]	Data Security Officer
P10 [B]	Director Tax application
P11 [B]	CISO
P12 [B]	Head Enterprise Architecture
P13 [C]	Chief Security Advisor

In accordance with the research question, we focused our interviews on the following topics:

What cloud computing challenges could be solved with innovative security technology in your company?

What is the current perception of the usefulness of TEE (confidential computing) in your company (sector)?

What are the perceived challenges of TEEs (confidential computing) in your company (sector)?

We classified the insights from the interviews based on the TOE framework. The main determinants are shown in Figure 2 and described afterward.

4.1. Technological Context

Compatibility with Existing Systems and Processes. Interview participants P1 [L] and P4 [L] both mentioned that the potential impact of adopting TEEs to their backup plans and storage solutions would need to be assessed.

"If I use this for [existing business] operations, it would be good to have this as an enterprise feature, without additional work from our side." (P1 [L]).

Interview participant P13 [C] mentioned that he sees a challenge in the need to refactor current applications, which would disrupt current operations.

"You have to refactor existing applications, which blocks many customers from using it." (P13 [C]).

Interview participant P13 [C] mentioned that not all processes could be executed with this technology, as performance is insufficient.

"Performance is also a problem if you think about working with a whole data lake." (P13 [C]).

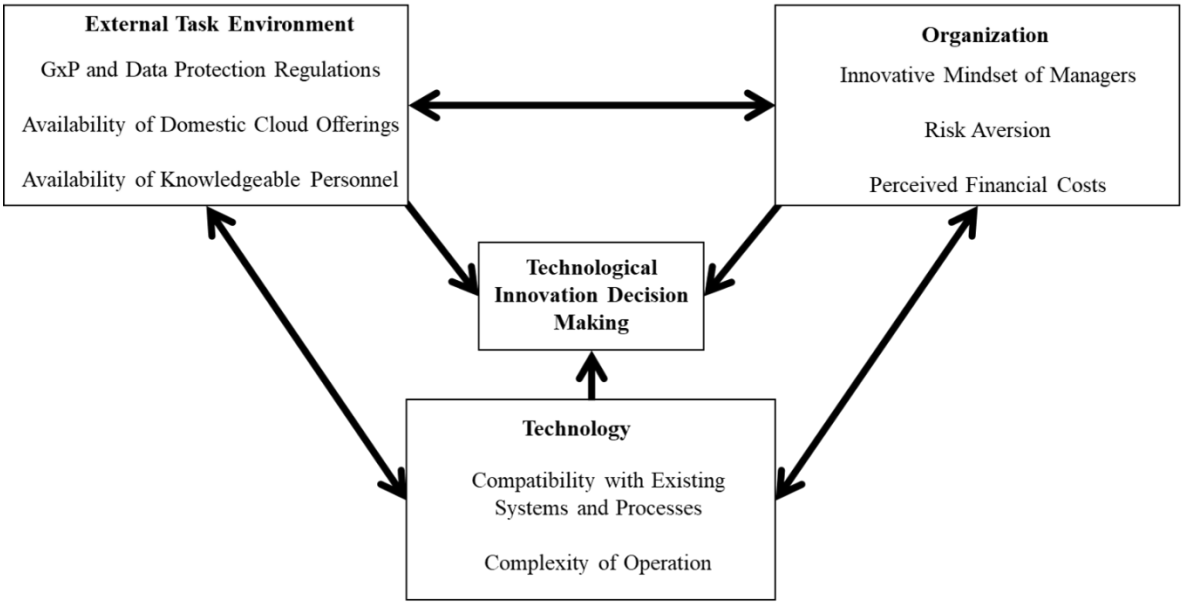

Figure 2*:* Perceived factors influencing the adoption of TEEs from the three perspectives of the TOE framework [3].

Complexity of Operations. Interview participant P1 [L] stated that the complexity of business operations is an essential factor.

"But it's also a matter of operational complexity as well as the know-how needed to operationalize this on a large scale." (P1 [L]).

Other interviewees mentioned that the complexity could increase due to additional security technology. They had already experienced this with other security technologies and observed a tradeoff between security and operational complexity.

"There will be a tradeoff between security and getting work done." (P7 [H]). "It is still too early to determine if this technology is usable on an everyday basis." (P10 [B]).

In addition, participant P13 [C] mentioned that most of the complexity could, in future, be reduced by the cloud provider so that a health care provider could focus on its core business.

"The focus of cloud providers is to run a secure IT environment. From our innovation, all customers can profit. The hospital should [easily use it] and take care of a patient and provide medical services." (P13 [C]).

4.2. Organizational Context

Innovative Mindset of Managers. Interview participant P3 mentioned that in the life sciences industry, managers are not focused on IT or innovation.

"We have no pressure to be innovative within the IT department" (P6 [H]).

Later on in the interview, he mentioned that the current mindset of managers would hinder the adoption of new technologies as the life sciences industry is generally conservative.

"Therefore, we use only well-established technologies." (P6 [H]).

Interview participants P4 [L] and P6 [H] stated that it is difficult and unnecessary to be pioneers in the life sciences and health care sectors.

"The health sector as a whole is defensive concerning innovation." (P9 [H]).

Interview participant P2 [L] stated that it is challenging to innovate in areas with a link to machines validated according to good manufacturing practices regulation (GMP) because such innovations require validation. Interviewee P12 [B] added that the adoption of new technology is not usually innovation-driven but regulation-driven.

"I think that in the banking sector, adoption doesn't happen if it is not required by the regulator." (P12 [B]).

Interview participant (P10 [B]) mentioned that innovation could be specific to departments within a

bank, but the core business is typically not an early adopter of innovations.

Risk Aversion. Interview participants P1 [L], P2 [L], and P4 [L] specifically mentioned the potential security gains from confidential computing as an attraction. According to participant P3 [L], risk aversion is a major organizational factor. He later added that the effort and resources required to adopt TEEs are difficult to estimate and might not be worth the risk reduction to his companies. Interview participants (P6 [H]) and (P7 [H]) pointed out that the security of patient data always comes first, and the loss of such data would lead to a high reputational damage.

"The safety of patient data always comes first." (P6 [H]). *"The reputational damage would be massive if patient data were leaked"* (P8 [H]).

Interviewee P12 [B] mentioned that the cybercrime risk would increase in the future, leading to a higher adoption rate of confidential computing. He added that it is also essential for security gains to be evidenced and trustworthy, as any breach would impact many customers.

"The whole field of cybercrime will increase, which could drive confidential computing and confidential data processing" (P12 [B]). *"If such a technology were adopted, there must be no systematic problems; otherwise a whole range of customers would be at risk"* (P12 [B]).

Interview participant P12 [B] mentioned that he still has to trust the final product developed with confidential computing. He was also undecided concerning risk mitigation based on technological guarantees.

"The system will be a little better, but there are still people involved, which always carries a risk. […] I have to be able to trust the final solution." (P12 [B]).

Interview participant (P13 [C]) saw a clear benefit from this technology, as it enables the cloud provider to prove that stored data cannot be accessed. This might persuade companies from regulated industries to use cloud services for sensitive data.

"For us as a cloud provider, it can help to prove that we are not accessing our clients' data" (P13 [C]).

Financial Costs. Interview participant (P13 [C]) mentioned that, currently, many risks are already accepted. Consequently, it is questionable whether the business would pay for technological mitigation of an already accepted risk.

"There has to be a business need […] a lot of risks we have already accepted, which could be mitigated by confidential computing." (P13 [C]).

Interview participant P4 [L] spoke of the potential cost of deploying and maintaining confidential computing.

"Above all, I wonder about the cost. Is this something that you pay for when using?" (P4 [L]).

4.3. Environmental Context

GxP Regulations. A host of regulations exist in the life sciences industry, summarized as GxP (good practices in process x). Interview participant P1 [L] perceives regulatory pressure as a driver for new security technology in his sector.

"I think the regulations will become tougher, and I am certain of that. Modern security concepts will kick in. Also, for things like this [confidential computing], sooner or later it will be required." (P1 [L]).

GxP regulatory requirements oblige the life sciences community to ensure their GxP-relevant data is sound. Many interviewees participants mentioned data integrity when discussing examples of encrypted data-sharing within pharmaceutical chains, TEE use-cases, or other innovations. In addition, statements of two interviewed decision makers underline the importance of proper data integrity mechanisms to ensure that regulatory auditors can perform their inspection on GxP regulations.

"A big challenge here is data integrity and data confidentiality […] It's important that someone has the key in case it has to be reconciled by the FDA." (P1 [L]).

Data Protection Regulations. There was a clear focus on the General Data Protection Regulation (GDPR) [24] during interviews with life science partners. In addition, those from the banking sector mentioned banking regulations as an important factor.

"I think the biggest hurdle is still the regulator [with regard to the Swiss Financial Market Supervisory Authority]." (P12 [B])

Three decision-makers cited challenges arising from GDPR in their recent innovation projects, such as the move to the cloud – and that such challenges could be solved through encryption alternatives such as TEEs. When discussing moving data to the cloud in the form of a data lake, interview participants P2 [L], P6 [H], and P8 [H] mentioned that data access restrictions need to be configurable in a role-based fashion, similar to ERP systems.

"It's important which data we can see as a company and which data are relevant to us" (P1 [L]). *"The electronic patient record can benefit if the data access can be secured on case level. A medical doctor treating a knee injury does not need to know the entire patient health record."* (P8 [H]).

However, several decision-makers were not able to think of a use-case where TEEs could improve compliance with privacy laws because their understanding of encrypted personal data is, for the most part, the same as for pseudonymized personal data. In this regard, they perceive TEEs only as an incremental improvement.

"I think because of the GDPR requirements, most of the personally identifiable information in our systems is already masked." (P5 [L]).

Interview participant P4 [L] explained that during their company's recent move to a total cloud environment, they had experienced a lot of GDPR-related challenges. For example, interview participant P4 [L] later explained that encrypted data is still deemed personally identifiable information. Interview participant P5 [L] and P6 [H] stressed the importance of masking personally identifiable information in line with data protection regulations.

"If we transfer data to the outside, we anonymize it." (P6 [H]).

Availability of Domestic Cloud Offerings. Several participants mentioned the importance of the data storage location. It is crucial for highly regulated companies operating in Switzerland to store their data in the country for security and privacy purposes. *"We have a clear policy regarding data storage. It has to be in Switzerland. Also, the encryption keys should be handled only in Switzerland." (P6 [H]).*

"For Swiss clients it's relatively important where their data is stored. Especially with the data protection law […] and I think this will increase the acceptance rate of the cloud" (P2 [L]).

Interview participant P9 also mentioned that operations in the Middle East face the same hurdles as in Europe.

"In the Middle East [where we also operate], there is a regulation that prohibits the transfer of data to foreign countries." (P9 [H]).

Availability of Knowledgeable Personnel. Interview participants P1 [L] and P12 [B] stated in detail that the availability of knowledgeable employees would be a determinant in deciding whether to adopt TEEs.

"But it's also a thing of […] the know-how that is needed to operationalize this en masse. […]proof of concept would need to be done first where […] the know-how that already exists in this area [has to be identified]. It is not sufficient if just one of our admins and one person at the outsourcer has an idea of how it works. There must be enough know-how on the market to operate and implement this." (P1 [L]).

"I think adoption is highly related to knowledgeable personnel. […] only then will a company trust a new solution." (P12 [B]).

Interview participant P13 [C] mentioned the associated risks arising from a lack of staff with knowledge of confidential computing.

"For users of this technology, it has to be clear that you have to be careful with your credentials because if you lose these, additional encryption cannot help." (P13 [C]).

5. Discussion

The insights from our interviews offer an impression of the organizational perception of TEEs within three highly regulated industries. They reveal that these companies will consider the further adoption of cloud technologies in light of the cost pressures within their industries. Furthermore, a sufficient understanding of TEEs does not yet exist within most companies interviewed. Indeed, they even perceive a lack of knowledge within their industry, which may hinder translating new TEE technology from theoretical implementation scenarios to practical commercial application. As practical instances of TEE still rare, this observation is unlikely to be limited to our observed industries. Therefore, we see this sociotechnical challenge as an important novel finding of our study. It seems to us that technology providers and academia should further focus on educating potential business users. This situation is not hugely different from the early days of blockchain technology [5]. Broadening the developer community could also close the current knowledge gap perceived by market participants. Current research on security technologies also supports our findings, as it suggests that lack of organizational readiness is one of the factors that can negatively influence the adoption of security technologies [15].

A second important finding is that TEEs are currently not a significant issue for regulated industries in Switzerland since they perceive no regulatory benefit. Instead, the technology is seen as an incremental improvement. The interviewees stated that their respective industries are guided by traditional values and are not focused on innovation because of current regulations. Based on these results, we see a need to understand better the impact of TEEs on data protection regulation. It is also worth noting that the literature still provides no clear picture of the regulatory effects of TEEs [1]. Work by Singh [23] suggests that TEEs could potentially be used for future business innovations and specific high-value sensitive data to comply with the security aspects of GDPR. Without explicit consent about the influence of TEEs on "(a) the

pseudonymization and encryption of personal data" [24], its adoption rate will, potentially, remain low.

As an additional insight the importance of domestic cloud offerings for regulated industries was identified within this study. Of course, cloud service providers can offer TEEs, but companies like Microsoft have only recently started offering Switzerland as a service location. We suggest this may hold for other countries too, giving cloud providers an incentive to provide domestic TEE offerings.

An added security gain itself is a core feature of the technology, and the perceived security gain is also shown as a general driver in the adoption of security technology [15]. However, the security guarantees offered by TEEs are controversial [7]. The sectors we examined traditionally have an aversion to risk where data and confidentiality are concerned. Our study confirms that there is no clear consent on the security benefits. Several participants see additional security gains but are also undecided whether TEE products offer higher security guarantees overall. At the moment, it seems that this proof must be provided on a case-by-case basis. In these cases, cloud adoption would no longer be hampered by security risks, and previous research regarding this factor should be reevaluated.

Very recently published literature highlights that compatibility with current operations is a vital adoption factor [15]. Within the context of regulated companies, we could verify these factors through our interviews. Although the complexity of TEEs was also mentioned in several instances, researchers are undecided about the influence this factor has on adoption [15]. Cloud service providers are starting to offer out-of-the-box confidential computing (TEE-based) through virtual machines [12]. Indeed, today's major cloud providers already offer trusted enclave functionalities within their infrastructure services [22]. This is a strong indication that cloud service providers will widely adopt TEEs. If this is the case, TEE utilization could be one additional cost element in the cloud service contract, and this would resolve complexity and compatibility issues in the future.

6. Outlook

To our knowledge, this is the first study that provides an organizational perspective on TEEs within the context of regulated industries. A possible step for future researchers would be to study less-regulated sectors and include companies from other countries. The perceptions of these organizations would undoubtedly augment our findings. Furthermore, it would be interesting to conduct a quantitative study with adopters and non-adopters of TEEs regarding the factors identified in this study. Such a study could quantify the importance of these factors and give hints about their interaction. It may be too early to find a statistically relevant sample; however, it would still be worthwhile to determine whether adopters view specific factors as more significant than non-adopters or vice-versa. Such findings would be able to substantiate further the groundwork presented in this study. As TEEs become more widely known, their potential will become more apparent. Notwithstanding, we believe that an early organizational assessment will improve their usefulness for industry practitioners.

7. Acknowledgment

The authors of this research paper were supported by Innosuisse, Grant Nr: 48335.1 IP-ICT. The authors would like to thank all the interview participants and the valuable feedback of the anonymous reviewers.

8. References

[1] Agrawal, N., R. Binns, M. Van Kleek, K. Laine, and N. Shadbolt, "Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation," Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM (2021), 1–13.

[2] Arnautov, S., B. Trach, F. Gregor, et al., "SCONE: Secure Linux Containers with Intel SGX," PROCEEDINGS OF OSDI'16: 12TH USENIX SYMPOSIUM ON OPERATING SYSTEMS DESIGN AND IMPLEMENTATION, USENIX Assoc; ACM SIGOPS (2016), 689–703.

[3] Baker, J., "The Technology–Organization–Environment Framework," In Y.K. Dwivedi, M.R. Wade, and S.L. Schneberger, eds., Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1. Springer, New York, NY, 2012, 231–245.

[4] Bogner, A., B. Littig, and W. Menz, Interviewing Experts, Springer, 2009.

[5] Conte de Leon, D., A.Q. Stalick, A.A. Jillepalli, M.A. Haney, and F.T. Sheldon, "Blockchain: properties and misconceptions," Asia Pacific Journal of Innovation and Entrepreneurship 11(3), 2017, pp. 286–300.

[6] Costan, V., and S. Devadas, "Intel SGX Explained," IACR Cryptol. ePrint Arch., 2016.

[7] Costan, V., I. Lebedev, and S. Devadas, "Secure processors part II: Intel SGX security analysis and MIT sanctum architecture," Foundations and Trends, 2017.

[8] Ermakova, T., B. Fabian, and R. Zarnekow, "Improving Individual Acceptance of Health Clouds through Confidentiality Assurance," Applied Clinical Informatics 7(4), 2016, pp. 983–993.

[9] Fernandez, E.B., R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems," Requirements Engineering 21(2), 2016, pp. 225–249.

[10] Framner, E., S. Fischer-Hubner, T. Loruenser, A.S. Alaqra, and J.S. Pettersson, "Making secret sharing based cloud storage usable," Information and Computer Security 26(5), 2019, pp. 647–667.
[11] Fu, Y., E. Bauman, R. Quinonez, and Z. Lin, "SGX-LAPD: Thwarting Controlled Side Channel Attacks via Enclave Verifiable Page Faults," In M. Dacier, M. Bailey, M. Polychronakis and M. Antonakakis, eds., Research in Attacks, Intrusions, and Defenses (raid 2017). Springer International Publishing Ag, Cham, 2017, 357–380.
[12] Gjerdrum, A.T., R. Pettersen, H.D. Johansen, and D. Johansen, "Performance of Trusted Computing in Cloud Infrastructures with Intel SGX," CLOSER: PROCEEDINGS OF THE 7TH INTERNATIONAL CONFERENCE ON CLOUD COMPUTING AND SERVICES SCIENCE, (2017), 668–675.
[13] Harnik, D., E. Tsfadia, D. Chen, and R. Kat, "Securing the storage data path with SGX enclaves," arXiv preprint arXiv:1806.10883, 2018.
[14] He, L., F. Huang, J. Zhang, et al., "Dynamic Secure Interconnection for Security Enhancement in Cloud Computing," International Journal of Computers Communications & Control 11(3), 2016, pp. 348–357.
[15] Herath, T.C., H.S.B. Herath, and J. D'Arcy, "Organizational Adoption of Information Security Solutions: An Integrative Lens Based on Innovation Adoption and the Technology- Organization-Environment Framework," ACM SIGMIS Database: the DATABASE for Advances in Information Systems 51(2), 2020, pp. 12–35.
[16] Hetzelt, F., and R. Buhren, "Security Analysis of Encrypted Virtual Machines," arXiv:1612.01119, 2017.
[17] Machida, T., D. Yamamoto, I. Morikawa, H. Kokubo, and H. Kojima, "A Secure Framework for User-Key Provisioning to SGX Enclaves," In L. Barolli, N. Kryvinska, T. Enokido and M. Takizawa, eds., Advances in Network-Based Information Systems, Nbis-2018. Springer International Publishing Ag, Cham, 2019, 725–732.
[18] Matetic, S., M. Schneider, A. Miller, A. Juels, and S. Capkun, "DELEGATEE: Brokered Delegation Using Trusted Execution Environments," PROCEEDINGS OF THE 27TH USENIX SECURITY SYMPOSIUM, Usenix Assoc (2018), 1387–1403.
[19] Mohamed, I., G. Marthandan, M. Norzaidi, and S.-C. Chong, "E-commerce usage and business performance in the Malaysian tourism sector: Empirical analysis," Inf. Manag. Comput. Security 17, 2009, pp. 166–185.
[20] Nilsson, A., P.N. Bideh, and J. Brorsson, "A Survey of Published Attacks on Intel SGX," Lund University, 2020, p. 12.
[21] Ramdani, B., P. Kawalek, and O. Lorenzo, "Predicting SMEs' adoption of enterprise systems," Journal of Enterprise Information Management 22(1/2), 2009, pp. 10–24.
[22] Rashid, F.Y., "The rise of confidential computing: Big tech companies are adopting a new security model to protect data while it's in use", IEEE Spectrum 57(6), 2020, pp. 8–9.
[23] Singh, J., J. Cobbe, Do Le Quoc, and Zahra Tarkhani, "Enclaves in the Clouds", 2020.
[24] THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, "General Data Protection Regulation (GDPR) – Official Legal Text", General Data Protection Regulation (GDPR), 2016. https://gdpr-info.eu/
[25] Tornatzky, L.G., and M. Fleischer, The Process of Technological Innovation, Lexington Books, Lexington, MA, 1990.
[26] Valadares, D.C.G., N.C. Will, J. Caminha, M.B. Perkusich, A. Perkusich, and K.C. Gorgônio, "Systematic Literature Review on the Use of Trusted Execution Environments to Protect Cloud/Fog-based Internet of Things Applications," IEEE Access, 2021, pp. 1–1.
[27] Wang, Y.-M., Y.-S. Wang, and Y.-F. Yang, "Understanding the determinants of RFID adoption in the manufacturing industry," Technological Forecasting and Social Change - TECHNOL FORECAST SOC CHANGE 77, 2010, pp. 803–815.
[28] Webster, J., and R.T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly 26(2), 2002, pp. xiii–xxiii.
[29] Martín-Martín, A., E. Orduna-Malea, M. Thelwall, and E. Delgado López-Cózar, "Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories", Journal of Informetrics 12(4), 2018, pp. 1160–1177.