Towards More Secure and Data Protective Intelligent Infrastructure Systems

Mariia Bakhtina[1]

[1]University of Tartu, Narva mnt 18, Tartu, 51009, Estonia

Abstract

With the megatrends of hyperconnectivity, the information systems transform into intelligent infrastructure (II) systems that allow data-based decision-making based on data processing. While the real-world use cases of II systems are just emerging and still are under active research and development, the problem of methods for information security and privacy protection in such SoSs is even more under-researched. As a result, there is a gap in the knowledge base in the guidelines on how information security officers should anticipate required changes to the organisation's information security strategy and formulate new plans, in case the organisation transforms its IT system towards the II system. In this research project, we want to create guidelines on how security risks and privacy protection should be managed in complex intelligent infrastructure systems. In this paper, we present the context of the PhD research work, research questions, the methodology and expected contributions of the study.

Keywords

Information security, privacy, identity management, system of systems, intelligent infrastructure

1. Introduction

With the global megatrends of hyperconnectivity [1, 2] and the need for super platforms (i.e. super apps) of the growing up Gen Z population [3], the *System of Systems (SoS)* become more relevant and ubiquitous than ever. In the classical definition, a system of systems refers to systems which were initially composed independently, but which act jointly toward the common goal through the synergy between them [4]. Meanwhile, *hyperconnectivity* means "the connectivity and interaction of everything that exists in digital environments, including systems, devices, objects, things, processes, activities, people, and data" [5].

In practice, there are a number of SoSs which enable hyperconnectivity. The implementations vary from the Internet of Things (IoT) and smart devices used by the end consumers, followed by Industry 4.0 and by the intelligent infrastructure (II) systems across industries (e.g., e-government, transportation, healthcare) where organisations' information systems are interacting with each other to enable collaboration between stakeholders. Such heterogeneous systems connectivity enables new data flows, which, in turn, allows data-based decision-making based. On the other hand, it also opens new attack vectors to the systems and to the security and privacy of manipulated information [6, 7] because of the non-compositional nature of SoS.

Proceedings of the Doctoral Consortium Papers Presented at the 35th International Conference on Advanced Information Systems Engineering (CAiSE 2023), June 12–16, 2023, Zaragoza, Spain

mariia.bakhtina@ut.ee (M. Bakhtina)

0000-0002-0940-9713 (M. Bakhtina)

CEUR Workshop Proceedings (CEUR-WS.org)

Thus security of each component in the intelligent infrastructure does not refer to the security of the whole SoS. As much as each separate system managed by the organisation should have its security and privacy objectives, additional information security and privacy management measures of the intelligent system as a whole must be in place. While the traditional security risk management approaches have been used for ages but mostly applied for the closed, one-purpose non-dynamic information system, there is a gap in validating their utility and effectiveness in developing complex SoSs. Currently, the real-world use cases of hyperconnected systems of systems are just emerging and still are under active research and development, the problem of methods for information security and privacy protection in such SoSs in the context of high attention to privacy and trust is under-researched. As a result, there is a gap in the knowledge base in the guidelines on how information security officers should anticipate required changes to the organisation's information security strategy and formulate new plans [8] in case the organisation transforms its IT system towards II system.

In this paper, we present a research plan to define the knowledge database by investigating the following research question (RQ): *How can security risks and privacy leakage be managed in intelligent infrastructure systems*? Our research considers an *intelligent infrastructure system* as a system of systems that may be composed of heterogeneous components and where each sub-system or component has its own scope of functionality and information processes while their composition enables delivering new value proposition to end users thanks to the enabled information flows. By answering this question, the PhD project aims to develop recommendations on managing information security and data privacy in II systems to help information security specialists in II industries to conduct their key tasks.

The paper is structured as follows. Sec. 2 described the problem areas addressed in the PhD research. Sec. 3 review the related work. Sec. 4 presents the research questions, the research approach, and the current state of the research. Finally, Sec. 5 concludes the paper.

2. Problem Statement

This research is composed of three studies that investigate different facets of II SoS and corresponding problem areas. The first problem area concerns the basic assumptions of the cooperation between systems in the II system. Specifically, the question of trust between cooperating stakeholders and systems is one of the fundamental corners stones. Trust is an assumption based on which systems and organisations decide which systems are trustworthy to communicate with [9]. Depending on the selected root of trust, systems may rely on different identity management systems. Thus, for emerging II systems, it is vital to understand which of the existing trust models is the most appropriate and upon which identity management system to build the collaboration [10, 11]. Moreover, the properly selected trust model and identity management system have a direct impact on the II system acceptance, as the trust of end users in the system is, to a large extent, defined by their awareness and belief that the system delivers an acceptable level of security and privacy protection for their data [12].

The second problem area concerns assuring the privacy of personal data and protection of organisations' sensitive data in the II systems (IISs). The transformation from a few separate systems which exchange valued data internally towards the exchange of such data between

systems inside the IIS tightens connections and blurs systems' boundaries. The connections of systems to enable cooperation in IISs involve reliance on collaborative data processing and management [13]. However, sometimes exchanged data may include (part of) sensitive personal data or sensitive organisational data. So here comes the question of finding the trade-off between the benefits of data sharing and the risks of sharing sensitive data or too much data, which can be reconstructed to reveal some sensitive data (i.e. privacy leakage) [13, 14].

Finally, the third problem area originates in the current maturing of the II systems, the growing number of implementations and system designs. While the II systems are becoming a reality and are used across industry domains (including smart parking solutions, e-government services, e-grids, and smart wearables in e-health) and geography, the development and usage of such innovative systems reveal new security and privacy management risks and challenges [15, 16]. For example, researchers highlight [17] that when II systems are built based on the existing disintegrated standalone systems where security measures were separately managed, their connectivity results in the lack of consistency and coordination in security measures, scattered around systems users' identities which causes impediments to the system usability. Moreover, the new information flows and tighter interaction points between systems most certainly change the risk profile, and the security and privacy measures which were used before transformation may become outdated and not effective. To this end, we see the gap in research on how the transformation of the information security management system (ISMS) progresses in the IISs and which aspects of security and privacy management are the most challenging.

3. Related Work

3.1. Identity management

Nowadays, intelligent infrastructure systems are developed based on the existing standalone information systems thanks to their interoperability characteristics or through using data exchange layers [17, 18]. Therefore, it is natural that the identity management (IdM) system used in the traditional information system, which is based on the public key infrastructure (PKI), will be inherited in II SoS. However, centralised PKI is prone to a single point of failure.

Currently, researchers investigate the advantages of self-sovereign identity (SSI), which is an alternative to the centralised trust model. In [19, 20], the SSI usage is researched primarily by showing the feasibility of SSI application for system end users and highlighting the advantages of blockchain for IdM. Other research [10] acknowledge that SSI is an effective way of managing digital identities and assuring data protection. Our research differs from the existing work by the context - namely, the identity of a legal entity, which contributes to the existing knowledge body by investigating how organisations' identity management differs from end users' identities.

3.2. Privacy analysis

Data leakage is the release of sensitive data to an untrusted environment. One of the ways to regulate and push organisations to prevent data leakage is the introduction of privacy regulations (e.g., GDPR in the EU). Thus, regulations force organisations to comply with their requirements. In [21], the authors proposed a method for model-driven compliance checks with

GDPR. However, they focus on assessing the text of privacy policies only, which may not reflect the full process during which the data is manipulated. A legal-URN framework is proposed in [22] for checking the legal compliance of business processes, but it implies developing a goal model for the European regulation by the tool user from the very beginning. Most of the other available tools for privacy conduct exclusively the analysis of a single mobile application and detect data leaks there. The closest to our research is work in [23], where authors propose a method for privacy analysis in IoT applications by applying a number of assessment methods.

3.3. Current state and challenges in the II system implementations

To develop the recommendations for the developing II industry on measures of information security and privacy management, the current gap and challenges faced by the companies in II while developing,managing, and using the II SoSs should be identified. To the best of our knowledge, there are no existing studies which have approached such gaps at the time of writing. The closest studies are the following two [24, 25]. In [24], the authors conducted an SLR of information security and privacy in intelligent railway systems. The authors identified the state-of-the-art research directions. Additionally, they classified existing challenges and solutions related to information security and privacy, which are addressed by the research considering technical, social, regulatory and ethical approaches. Similarly, in [25], the authors reviewed the knowledge body about security and privacy challenges in smart cities. The study resulted in the identified security and privacy concerns and threats grouped by the smart city operation areas and the open challenges in these areas. The study also mapped the existing protection technologies to smart cities' security and privacy areas. Our research is similar in the way and goals of literature sources identification, but in our study, we will have a broader focus and use the information security frameworks for guiding data extraction and analysis that additionally consider the organisational and strategical dimensions. In contrast to the related work, we also aim to identify the current state of regions and compare it with state-of-the-art research to pinpoint areas where research findings do not find their way to real-life solutions.

3.4. Recommendation on managing information security and data privacy

ENISA [26] in its guidelines for security IoT defined a mapping of good practices that shape objectives of actors involved in the IoT supply chain regarding the most relevant cyber security threats for the specific supply chain stage. The guidelines are also supported with a summary of the most relevant security standards, which should help with defining measures to fulfil good practices. The current study aims to deliver the analogue contribution but for the actors that rely on the connected, intelligent infrastructure systems, which are mainly presented by the connected information systems rather than resource-constrained IoT devices.

4. Research Approach and Contributions

In our research, we address each problem area described beforehand separately, and consolidate the separate findings into the final set of recommendations (see Fig. 1).

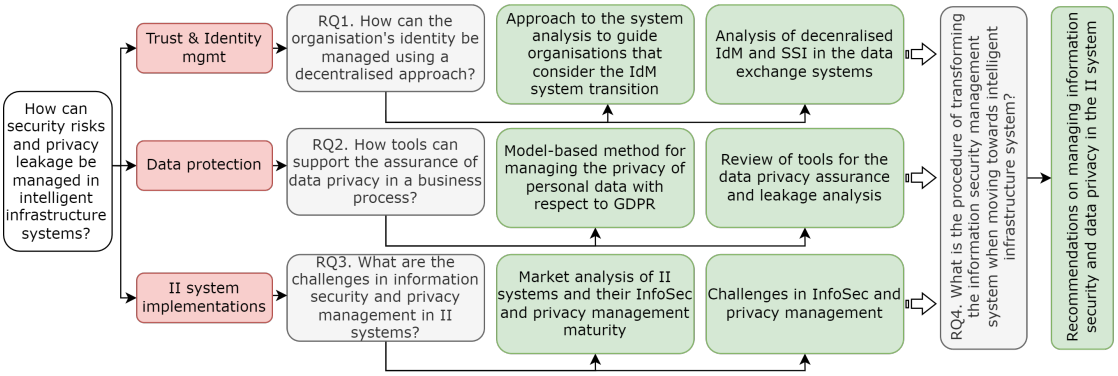

Figure 1: Thesis structure

Each of the three studies has its own research method with evaluation, while the fourth study aims to validate the aggregated results from the first three studies and design the recommendation based on the developed before artefacts and findings. The PhD research should result in an overview of state-of-the-art means (policies, approaches, methods, techniques, and tools) for II systems protection accompanied by recommendations on how to approach information protection when transforming your business and IS into an II system. The following section describes how each research area is approached and reports on the current progress.

4.1. Identity management and SSI - Case of distributed data exchange systems

This exploratory study aims to investigate the usage of the emerging concept of self-sovereign identity (SSI) and its effect on security and privacy management. In particular, the research aims to scrutinise the feasibility of a decentralised PKI approach for organisations' identity management (IdM) in data exchange systems.

Method. The research sub-question (RQ_1) of this study sub-project is as follows: *how can the organisations' identity be managed using a decentralised approach?* We follow the design science approach [27] to solve the business problem for the X-Road data exchange system. X-Road serves as the backbone of the Estonian, Icelandic (and a few other countries) digital government infrastructures. Based on the selected system, we developed artefacts for the transition to the decentralised IdM approach. To validate the artefacts, we are working on the proof-of-concept, which will help assess the feasibility and quality of the decentralised approach compared to the centralised one. This allows us to reveal the advantages and limitations of using decentralised PKI based on the blockchain for managing organisations' identities. The first cycle of testing revealed the need for extending the artefacts with the design on the organisation's identity wallet management. Therefore, we also investigate the usage of smart cards and hardware wallets for managing the keys of organisations' identities. Thus, we explore how employees' personal wallets could be used for the delegation of operations on behalf of the organisation.

Current progress. So far, we have developed an architecture for the data exchange system enabled by decentralised PKI processes of managing members [28]. In [29], we propose an approach of system analysis that should guide organisations that considers the transition to decentralised identity management. Currently, we are testing the developed artefacts through the proof-of-concept implementation.

4.2. Privacy leakage analysis

In the second study sub-project, we investigate how to prevent privacy leakages (including leakage of personally identifiable data as well as the organisation's confidential data). The study's primary goal is to identify and assess the existing state-of-the-art tools which organisations could use as a part of their tool sets for ensuring sensitive data privacy in a business process with collaborative data processing.

Method. The research question (RQ_2) of this part of the PhD study is as follows: *how can tools support the assurance of privacy in a business process?* First, we investigate the existing tools which help to define requirements for privacy assurance of personal data according to GDPR. Answering this question, we will have a defined procedure for elicitation of requirements to comply with the GDPR requirements. Second, we determine how tools help to compare the effectiveness of privacy-enhancing technologies in the business process context. Answering the second question, we will support the selection of technical measures for privacy assurance based on their effectiveness in protecting data objects from leakage.

Current State of the Research. So far, this part of the study has resulted in [30]. As the starting point, we selected the two tools: (i) DPO tool[1] for checking the compliance of a business process with the GDPR requirements, and (ii) Pleak tool[2] for detecting possible data leakages. In [30], we present a method for managing data privacy with respect to GDPR, which relies on the usage of the selected tools. The method's usability is validated by the experimental application of the method to a ride fulfilment process in a ride-hailing company enabled by an autonomous driving system. In the future, the proposed method will (i) undergo another round of validation to prove its usability by applying it to another use case of collaborative data processing, and (ii) be extended by comparing other existing tools for data privacy assurance.

4.3. Current state and challenges of the information security and privacy management in the II system implementations

The goal of this part of the PhD study is to identify the challenges of information security and privacy management in the selected domain of II, namely, intelligent transportation. The study aims to define which security and privacy standards are applicable in the selected industry, how they are practised, which information security and privacy management methodologies, tools and technologies they use during the intelligent system lifecycle. As a result, we plan to define

[1]DPO Tool can be accessed at https://dpotool.cs.ut.ee/
[2]Pleak can be accessed at https://pleak.io/

how mature is information security and privacy management in the companies of the selected region compared to the state-of-the-art solutions.

Method. To achieve our goal and answer RQ_3 (*What are the challenges in information security and privacy management in II systems?*), we plan to conduct an empirical study of sector analysis of the intelligent transportation systems in the selected regions. Thus, we will (1) define the state-of-the-art measures of information security and privacy management; (2) survey the companies (i.e. sector analysis) to compare their level of information security and privacy management maturity with the level of the state-of-the-art solutions.

First, the state-of-the-art measures will be defined based on the systematic literature review (SLR) following the corresponding guidelines [31]. For SLR, we use the following query: ("security" OR "privacy protection" OR "data protection") AND ("technologies" OR "measure")) AND (`Industry_name`), where instead of `Industry_name`, we use "vehicle sharing", "smart parking", "tool collection", and "traffic management" and their synonyms. From the selected papers, we extract policies, approaches, methods and techniques for information security and privacy management (referred to later as "measures"). The data from the SLR is organised in the four dimensions (processes, organisational design, people and technological solutions) based on ISACA's BMIS [32], McCumber's Cube [33] and RMIAS [34].

Second, the intelligent transportation sector companies should be surveyed using a questionnaire and interviews to identify their level of information security and privacy management maturity. The questionnaire and interviews are developed using the identified technologies and measures. The profile of the information security and risk management in the state-of-the-art and in each surveyed company should be created to characterise four dimensions.

Current progress. Based on the theoretical model for information security and privacy management and the results from the sector analysis, we will define the challenges in the selected industry. The challenges should guide future research directions to support a broad audience's development and acceptance of intelligent infrastructure. The identified gaps between state-of-the-art security and privacy states will be used as information materials for the sector companies to raise their awareness about the measures to be implemented to improve II systems.

4.4. Recommendation on managing information security and data privacy in II system

The goal of the final contribution is to help a chief information security officer (CISO) and cybersecurity architect in organisations using II SoS to conduct their key tasks defined in the European cybersecurity skills framework [8]. Specifically, we aim to help assess the organisation's cybersecurity posture when the organisation transforming their IT system towards intelligent infrastructure system by integration of IoT and with external ISs. As a result, CISO should have a guide on defining security requirements, goals and checking their alignment with the organisational objectives.

Method. To answer the research question RQ_4 (*What is the procedure of transforming the information security management system when moving towards an intelligent infrastructure sys-*

tem?), we will analyse the requirements for the security II systems identified in the previous contributions. Their consolidation should follow a structure similar to ENISA's guidelines [26] and map the actors of II system with the recommendations defining cybersecurity goals, requirements strategies and policies, aligned with a business strategy that aims to leverage hyperconnectivity through intelligent infrastructure systems usage. The recommendations development will follow the design science methodology [27] which includes the evaluation and dissemination steps as mandatory in the artefact design and problem addressing.

Current progress. This part of the PhD research study is based on the results from other research parts. Therefore, the progress in each of the studies discussed above contributes to scoping the problem and defining the objective of the solution.

5. Concluding Remarks

In this PhD research, we tackle the problem of assuring information security and data protection in the heterogeneous system of systems used as intelligent infrastructure for producing the public good for end users. Expected contribution includes revealing how security risks and privacy protection are managed in the complex intelligent infrastructure systems, what are the current challenges and how trust between the II sub-systems could be managed to promote the systems' acceptance and usability.

6. Acknowledgments

This Ph.D. thesis is supervised by Prof. Raimundas Matulevičius. This research is supported by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] Special Secretariat of Foresight (Hellenic Republic), Megatrends 2040. volatility, uncertainty, resourcefulness, https://foresight.gov.gr/en/studies/Megatrends-2040-Volatility-Uncertainty-Resourcefulness/, 2022.

[2] Strategic Futures Group of the National Intelligence Council (US), Global trends 2040: A more contested world, https://www.dni.gov/index.php/gt2040-home, 2021.

[3] Gartner, Top strategic technology trends 2023, https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023, 2022.

[4] C. B. Nielsen, P. G. Larsen, J. Fitzgerald, J. Woodcock, J. Peleska, Systems of systems engineering: Basic concepts, model-based techniques, and research directions, ACM Comput. Surv. 48 (2015). doi:10.1145/2794381.

[5] S. E. Bibri, Z. Allam, The metaverse as a virtual form of data-driven smart cities: the ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society, Computational Urban Science 2 (2022) 22. doi:10.1007/s43762-022-00050-1.
[6] N. Mexis, N. A. Anagnostopoulos, S. Chen, J. Bambach, T. Arul, S. Katzenbeisser, A lightweight architecture for hardware-based security in the emerging era of systems of systems, J. Emerg. Technol. Comput. Syst. 17 (2021). doi:10.1145/3458824.
[7] M. A. Olivero, A. Bertolino, F. J. Dominguez-Mayo, M. J. Escalona, I. Matteucci, Addressing security properties in systems of systems: Challenges and ideas, in: R. Calinescu, F. Di Giandomenico (Eds.), Software Engineering for Resilient Systems, Springer International Publishing, Cham, 2019, pp. 138–146.
[8] European Union Agency for Cybersecurity, ECSF, European cybersecurity skills framework, European Union Agency for Cybersecurity, 2022. doi:10.2824/859537.
[9] R. C. Mayer, J. H. Davis, F. D. Schoorman, An integrative model of organizational trust, The Academy of Management Review 20 (1995) 709–734.
[10] European Union Agency for Cybersecurity, E. Nikolouzou, V. Paggio, M. Dekker, Digital Identity: Leveraging the SSI Concept to Build Trust, Publications Office of the European Union, 2022. doi:10.2824/8646.
[11] D. Pöhn, P. Hillmann, Reference service model for federated identity management, in: A. Augusto, A. Gill, S. Nurcan, I. Reinhartz-Berger, R. Schmidt, J. Zdravkovic (Eds.), Enterprise, Business-Process and Information Systems Modeling, Springer International Publishing, Cham, 2021, pp. 196–211.
[12] M. N. Alraja, M. M. J. Farooque, B. Khashab, The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the iot-based healthcare: The mediation role of risk perception, IEEE Access 7 (2019) 111341–111354. doi:10.1109/ACCESS.2019.2904006.
[13] European Union Agency for Cybersecurity, Guidelines for SMEs on the security of personal data processing, European Network and Information Security Agency, 2017. doi:10.2824/867415.
[14] ISACA, Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges, white paper, Schaumburg, IL, USA, 2021.
[15] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevičius, A.-A. O. Affia, M. Laurent, N. H. Sultan, Q. Tang, Post-quantum era privacy protection for intelligent infrastructures, IEEE Access 9 (2021) 36038–36077. doi:10.1109/ACCESS.2021.3062201.
[16] D. Lopresti, S. Shekhar, A national research agenda for intelligent infrastructure: 2021 update, 2021. URL: https://europepmc.org/article/PPR/PPR274324.
[17] A. Ramtohul, K. M. S. Soyjaudah, Information security governance for e-services in southern african developing countries e-government projects, Journal of Science & Technology Policy Management 7 (2016) 26–42. doi:10.1108/JSTPM-04-2014-0014.
[18] J. Weber-Jahnke, L. Peyton, T. Topaloglou, eHealth system interoperability, Information Systems Frontiers 14 (2012) 1–3. doi:10.1007/s10796-011-9319-8.
[19] S. Feulner, J. Sedlmeir, V. Schlatt, N. Urbach, Exploring the use of self-sovereign identity for event ticketing systems, Electronic Markets 32 (2022) 1759–1777. doi:10.1007/s12525-022-00573-9.
[20] W. Fdhila, N. Stifter, A. Judmayer, Challenges and opportunities of blockchain for auditable

processes in the healthcare sector, in: BPM 2022 Blockchain, RPA and CEE Forum, Springer International Publishing, Cham, 2022, pp. 68–83.
[21] D. Torre, A. Mauricio, G. Soltana, M. Sabetzadeh, L. C. Briand, Model driven engineering for data protection and privacy: Application and experience with GDPR, CoRR abs/2007.12046 (2020b).
[22] S. Ghanavati, Legal-URN framework for legal compliance of business processes, Ph.D. thesis, University of Ottawa (Canada), 2013.
[23] B. Nazzal, M. H. Alalfi, An automated approach for privacy leakage identification in iot apps, IEEE Access 10 (2022) 80727–80747. doi:10.1109/ACCESS.2022.3192562.
[24] P. López-Aguilar, E. Batista, A. Martínez-Ballesté, A. Solanas, Information security and privacy in railway transportation: A systematic review, Sensors 22 (2022). doi:10.3390/s22207698.
[25] M. H. Panahi Rizi, S. A. Hosseini Seno, A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city, Internet of Things 20 (2022) 100584. doi:https://doi.org/10.1016/j.iot.2022.100584.
[26] European Union Agency for Cybersecurity, C. Skouloudi, R. Dede, A. Malatras, R. Naydenov, Guidelines for securing the internet of things : secure supply chain for IoT (2021).
[27] K. Peffers, T. Tuunanen, M. A. Rothenberger, S. Chatterjee, A design science research methodology for information systems research, J. Manag. Inf. Syst. 24 (2008) 45–77.
[28] M. Bakhtina, R. Matulevičius, A. Awad, P. Kivimäki, Rebooting Trust Management in X-Road, Public Report, Nordic Institute for Interoperability Solutions (NIIS), 2022.
[29] M. Bakhtina, R. Matulevičius, A. Awad, P. Kivimäki, On the shift to decentralised identity management in distributed data exchange systems, in: SAC '23: The 37th ACM/SIGAPP Symposium on Applied Computing, March 27-March 31, 2023, Tallinn, Estonia, ACM, 2023, pp. 864–873. doi:10.1145/3555776.3577678.
[30] M. Bakhtina, R. Matulevičius, M. Seeba, Tool-supported method for privacy analysis of a business process model, Submitted for publication, 2023.
[31] B. Kitchenham, S. Charters, Guidelines for performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE-2007-01, 2007.
[32] R. v. Roessing, The isaca business model for information security: An integrative and innovative approach, in: ISSE 2009 securing electronic business processes, Springer, 2010, pp. 37–47.
[33] J. McCumber, Assessing and managing security risk in IT systems: A structured methodology, Auerbach Publications, 2004.
[34] Y. Cherdantseva, J. Hilton, A reference model of information assurance & security, in: 2013 International Conference on Availability, Reliability and Security, 2013, pp. 546–555. doi:10.1109/ARES.2013.72.