Cloud Computing Adoption in Critical Infrastructures - Status Quo and Elements of a Research Agenda

Michael Adelmeyer[1], and Frank Teuteberg[1]

[1] Osnabrück University, Accounting and Information Systems, Osnabrück, Germany
{michael.adelmeyer,frank.teuteberg}@uni-osnabrueck.de

Abstract. Critical infrastructures, as the backbone of societal life, become increasingly dependent on IT. Thus, in order to ensure security and resilience, they face strict IT legislations and requirements. However, due to efficiency benefits, such as cost savings and increased flexibility, critical infrastructures increasingly adopt innovative IT models like cloud computing. This is despite the fact that migrating processes or systems into a cloud involves major risks for sensitive IT landscapes, since the control over data and security measures is delegated to cloud providers. In order to identify the current status quo of cloud computing in critical infrastructures, we conduct a systematic literature review, an analysis of cloud-based outsourcings of German critical infrastructures and expert interviews. Our findings provide an overview and a research agenda of cloud usage in critical sectors, which are helpful for critical infrastructure and cloud providers alike in order to adopt or manage cloud solutions.

Keywords: Cloud Computing, Critical Infrastructures, IT Security, IT Risks

1 Introduction

Critical infrastructures (CIs) take over a crucial public role, as they provide vital utilities. The German IT Security Law defines CIs as facilities, installations or parts thereof belonging to the sectors of energy, health, water, nutrition, information technology and telecommunications, transport and traffic as well as finance and insurance, which are of great importance for the functioning of the community because their failure or impairment would result in significant supply shortages or threats to public safety. As IT systems are an essential element of reliable service provisioning of CIs [1], CIs face stringent measures and legislations regarding security, privacy and resilience of their IT landscape [2, 3]. Due to the specific risks and requirements, CIs often host their own IT infrastructure or at most share resources with organizations with similar demands [4, 5]. However, due to manifold benefits, such as scalability, flexibility and cost reduction [6], CIs increasingly migrate IT services to cloud environments [2, 4, 7, 8]. Cloud computing is an operational model that provides on-demand access to a shared pool of resources, e.g. applications or hardware [6]. On the one hand, CIs are able to improve their resilience and availability with cloud solutions [8], recover faster in case of a failure [5] or benefit

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

from dynamic resource allocation and thus manage imponderable load peaks [9]. On the other hand, CIs face additional risks when moving IT systems or processes into a cloud [5, 10], such as the loss of control over security and privacy measures, data location, authentication and access control, third-party attacks or interferences, legislative issues or the violation of service level agreements (SLAs) [5]. The risks of deploying services into a cloud are difficult to assess, since cloud environments are opaque and often problematic to monitor [2]. This is especially challenging as CIs and therefore their cloud providers have to meet complex security and resilience requirements and demands of various stakeholders [10, 11]. Although the requirements are strict, existing cloud services fail to take proper account of these issues [2]. The pooling of computing resources in clouds even intensifies structural interdependencies and network risks between CIs and their cloud providers [12].

The IT security requirements of CIs and industrial stakeholders differ substantially and there are major differences even between the individual CI sectors [4]. Further, the risks vary depending on the selected cloud service and deployment model [13]. Existing literature mainly focuses on risks and corresponding standards but lacks an overview of the status quo of cloud usage in CIs. With the increasing adoption of cloud solutions in CIs, there is an urgent need to understand the differences regarding cloud service and deployment models as well as the involved sectors. Based on a systematic literature review, an analysis of outsourcings of German CI providers as well as expert interviews the status quo and a research agenda on cloud adoption in CIs are presented. Thereby, the focus is on systems, processes and functions, cloud service and deployment models, sectors as well as risks arising from cloud usage in CIs. The findings reveal that cloud computing is predominantly adopted in 'non-critical' areas of CIs. However, the use of public cloud or Software as a Service models is increasing. Both cloud providers and CIs need to understand the corresponding challenges, issues and risks in order to successfully adopt and manage cloud solutions. In this context, the research agenda determines future steps for science and practice alike, e.g. regarding risk management.

2 Research Approach

2.1 Literature Analysis

In order to provide an overview of the current state of research regarding the adoption of cloud computing solutions by CI operators, we conducted a systematic literature analysis following the approach of vom Brocke et al. (2009) [14]. The analysis of existing literature is an essential part of scientific work with the objective to elaborate the state of research in a certain field, to reveal possible knowledge gaps and motivate researchers to close these by identifying new research areas and directions. To cover the interdisciplinarity of the topic, we searched the databases AIS electronic library, EBSCOhost, ScienceDirect, SpringerLink, AIS Web of Knowledge and Google Scholar. For the queries, we used the keywords "critical infrastructure*" OR "critical national infrastructure*" OR "critical asset*" OR "critical system*" OR "critic*"

AND “cloud comput*” OR “cloud*” OR “outsourc*” and their German equivalents. We identified relevant publications by inspecting the titles, keywords and abstracts, which resulted in a total of 18 articles. Based on this result set, we conducted a forward and backward search, leading to seven further publications[1]. The majority of the literature found originates from conference proceedings. In order to identify the status quo, the publications were systematically examined using category building. As selection criteria, the different cloud service and deployment models, sector-specifics and risks were chosen. The results of the analysis serve as the basis for the status quo of cloud usage in CIs (cf. section 3) and the research agenda (cf. section 4).

2.2 Practical Analysis

To determine the current status quo in practice, we conducted an analysis of present outsourcings of German CIs to cloud services. In our search for CI providers and given the lack of appropriate public listings, we concentrated on the members of the working group UP KRITIS, a public-private cooperation between CI operators, their unions and governmental authorities. But here again no public list of the UP KRITIS members was available. Therefore, we examined the so-called “logo cloud”[2], in which the logos of the involved organizations can be registered upon request, in order to identify and categorize these CI operators. Since a distinct allocation of the companies to the aforementioned CI sectors of the German IT Security Law was not always possible, “mixed sectors” were defined. In this step, non-CI-providers like unions, governmental authorities and other stakeholders (e.g. cloud providers or certification authorities) were omitted, which led to the identification of 80 CIs[1].

In a next step, the identified CI operators were examined regarding the use of cloud technology. For this purpose, we considered business reports – as far as publicly available – as well as further information on cloud usage of the respective organizations from the internet, mainly from corporate websites. Subsequently, the previously determined sources for the adoption of cloud technologies of CIs were analyzed in detail. In this analysis, the focus was put on the use of cloud service [Infrastructure as a Service (IaaS), Platform as a Service (PaaS) Software as a Service (SaaS)] and deployment models (public, private, hybrid and community). In addition, the respective processes, systems or business functions, which are outsourced to or substituted by cloud technologies, were determined.

2.3 Expert Interviews

The results are further complemented by four expert interviews. Due to the relevance and novelty of an investigated subject, expert interviews can reveal information that is not yet available in scientific literature. The overall approach of the expert interviews can be summarized as follows [15]: on the basis of the literature analysis, a semi-

[1] A full overview of the identified publications, the examined critical infrastructure providers and the corresponding findings can be obtained at http://bit.ly/MKWI2018

[2] http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Logo_Cloud.pdf, *23.11.2017*

structured interview guide was developed containing eight interview questions that target the current use of cloud services, potentials, risks and open issues. After a pretest, the final interviews were conducted and qualitatively analyzed. The experts were employees of a CI and a consulting company (cf. Table 1).

Table 1. Experts Interviewed

ID	*Sector*	*Position/Function*
1	Transport & Traffic	Business Intelligence Architect
2	Transport & Traffic	Project Management
3	Transport & Traffic	Team Lead Application Development
4	Consulting	Senior Consultant, Security Analyst

3 Status Quo of Cloud Usage in Critical Infrastructures

3.1 Overview and Related Work

Although a plenitude of publications addresses cloud usage in specific industry sectors (e.g. finance [16]), only few articles approach the cloud domain from a CI perspective. Of the 25 publications identified the majority dates to the years 2013-2015 (19). A large part of the publications (8) treats security issues and risks related to the adoption of cloud services in critical infrastructures. For example, Younis et al. (2013) and Anastacio et al. (2013) provide an overview of risks and security measures for the deployment of CI components in a cloud [11, 17]. However, these publications often focus on general risks associated with cloud computing. A further major focus lies on regulatory aspects (7). In this context, Adelmeyer et al. (2017) illustrate IT risk management measures regarding the German IT security law [13]. Chochliouros et al. (2015), Paudel et al. (2014), Hudic et al. (2014) and Wagner et al. (2015) highlight various regulatory requirements and standards or guidelines for CIs, such as ISO 27001 [4, 5, 18, 19]. In addition, Wagner et al. (2015) point out that some security aspects are only inadequately addressed by existing standards and guidelines.

First major efforts to overcome the issues of cloud usage in CIs were undertaken by the EU-funded projects "SECCRIT" ("SEcure Cloud computing for CRitical infrastructure IT") with the objective to analyze and evaluate cloud related security risks for CIs [2–5, 8, 10, 20] and "CI2C" ("Critical Infrastructures and Cloud Computing"). Further, the European Network and Information Security Agency (ENISA) published a report that addresses cloud computing from a critical infrastructure information protection perspective with a focus on cloud scenarios and relevant threats [21]. However, the body of knowledge lacks a comprehensive current overview of the field. Thus, we analyzed the identified literature with regard to specifics concerning service and deployment models, functions, CI sectors and risks. Furthermore, as no empirical study on the use of cloud computing services in CIs could be identified, we conducted a practical analysis. At 18 of the 80 investigated CI operators, which approximate 22.5%, we found information on the use of cloud services. In contrast to the predictions of the ENISA, that states that around 80% of all

organizations will be dependent on cloud computing by today [21], the figure is relatively low. However, given the fact that we had to rely on publicly available information only, we assume the actual figure to be higher. In general, little information on the adoption of cloud technology was found in the business and annual reports, so that we had to rely on external sources, such as company websites. It was further found that many CIs simultaneously act as cloud operators and providers. In the following sections, the results of the literature and practical analysis as well as the expert interviews are presented. Table 2 summarizes the aggregated findings of the practical analysis. In total, we identified 23 cloud adoption cases at 18 CIs. However, not for every case we were able to distinctly identify a respective categorization.

Table 2. Aggregated Results of the Practical Analysis

Focus	*Cloud Adoption Cases (Quantity of Occurrence)*							
Systems/ Processes	Sales/ Distribution (7)	Data Center Operations (6)	Finance/ HRM (2)	E-Mail (2)	Software (1)	Unknown/ Others (5)		
Service Models	Software as a Service (13)	Infrastructure as a Service (5)	Platform as a Service (1)	Unknown/ Others (4)				
Deployment Models	Private Cloud (9)	Public Cloud (8)	Community Cloud (1)	Hybrid Cloud (0)	Unknown/ Others (5)			
Sectors	Energy (4)	Finance/ Insurance (4)	Energy/ Water (3)	Transport/ Traffic (3)	Water (2)	Nutri-tion (1)	IT & Telco (1)	

3.2 Systems, Processes and Functions

Regarding the systems, processes and functions of CIs that are outsourced to cloud services, only little information is available in the literature. In most cases, CIs are expected to replace 'non-critical' systems, processes or functions by cloud services [7]. In contrast to 'mission-critical' services, support systems and tertiary services can be provisioned via clouds more easily, especially when considering public cloud environments [22]. This finding coincides with the estimation of expert no. 4 that "the tendency for the adoption of cloud solutions in CIs is rising, but initially concentrates on non-critical areas". Thus, each CI has to individually evaluate every single migration to a cloud with a strong focus on security, availability and integrity [23]. However, with the increasing digitization, formerly isolated systems like Supervisory Control and Data Acquisition (SCADA) or industrial control systems that are widely used in CIs are moving to modern environments like clouds, which expose these systems to cloud-related threats [7, 23, 24]. The practical analysis revealed that sales/distribution (7 cases), including supply chain management, customer service, social media and invoice handling, followed by IT data center operations (6) are the most frequent areas for the adoption of cloud technology in CIs. However, information on outsourced systems, processes and functions is scarce (5 unknown/others), which demands for future research in this area. In summary, the analyses revealed that rather uncritical areas, e.g. sales/distribution, are major adoption areas for cloud technology in CIs.

3.3 Cloud Service Models

Depending on the deployment or service model of a cloud, the corresponding risks vary [13]. Thus, the different service models are associated with individual security requirements and threats [23, 25]. Following Diez and Silva (2011), the majority of CIs use SaaS or IaaS models for 'non-critical' business functions. Further, they state that SaaS offers the least control over the underlying cloud infrastructure, since this is fully delegated to the service provider [7]. As numerous SaaS providers rely on other cloud providers for fundamental resources such as PaaS or IaaS, the latter are seen as critical likewise [21]. The resulting interdependencies between organizations, service providers and users create network risks, as a failure of large cloud service providers would have a cascading effect on other CIs [19]. Thus, particularly IaaS and PaaS providers need to strengthen their resilience and security measures. The quantitative analysis of the service models used in practice revealed that SaaS is used most frequently (13), followed by IaaS (5) and PaaS (1). This distribution resembles the evaluation of the expert interviews. All four respondents indicated the frequent use of SaaS. In this context, especially public cloud SaaS solutions like Salesforce or Microsoft Office 365 (4 cases) are considered. Further, two experts pointed out adoptions of IaaS and one expert indicated a PaaS solution for test environments.

3.4 Cloud Deployment Models

As public clouds are difficult to monitor and control, prone to attacks, lack direct governance and have issues related to multi-tenancy and storage location [7], it is unlikely that CIs outsource core functions or services to public clouds [22]. Since in public and hybrid solutions the data is transferred to third parties, sufficient network and storage security measurements and assurances have to be implemented, to ensure the integrity and confidentiality of data outside of CIs' private IT landscapes [22]. In contrast, private clouds can be used for critical functions and systems that have to stay in-house. Private clouds grant full control over data management and security measures and thus allow for specific fail-safe or cluster mechanisms, which cannot be implemented in public solutions [7, 23, 25]. Further, private clouds can be used as a staged approach to a prospective shift to public environments [7]. However, the economies of scale and the elasticity and flexibility are lower. Since CIs, due to their specific risk exposures and requirements [4, 5], often host their own IT infrastructure or at most share resources with organizations with similar demands, community clouds seem to be an adequate solution [23]. As community clouds limit certain risks, e.g. related to multi-tenancy [7] or the prevention of external dependencies [26], they are suitable in case private clouds are too expensive and public clouds do not meet individual security demands. However, trust in other involved actors and organizations regarding data and environment security measures is crucial in such solutions [7]. Further, the protection of such CI community solutions against cyber-attacks is vital, since they constitute an attractive target for attackers [7, 23].

The investigation of the service and deployment models used in practice revealed that IaaS is most often implemented as a private cloud (4 cases) and SaaS solutions as

public (8) or private clouds (3). Considering all cloud deployments, private clouds were used most frequently (9), followed by public (8) and community clouds (1). Hybrid clouds were not identified. In this context, the cloud of the Deutsche Bahn was categorized as "others", as it is a virtual private cloud based on the open infrastructure of an external service provider that is protected by access restrictions. The experts stated that public clouds are used most frequently in combination with SaaS. Expert no. 4 outlined that it is "often a matter of price, since private clouds are more expensive". According to expert no. 2 there is a "need for combined and distributed architectures that enable the interaction of private and public clouds".

3.5 Sectors

IT environments of CIs are often heterogeneous, since they comprise various kinds of infrastructures and systems. Consequently, CIs have individual security requirements, even between the different sectors [11]. The majority of publications (17) does not provide any information or focus on specific sectors. Instead, only some unrepresentative examples for cloud adoption cases in various sectors are given (e.g. [11, 21]). Driven by the objective to provide more flexible services through the virtualization of their infrastructures, telecommunication operators were among the first to adopt cloud solutions [8, 23]. Also the energy sector is at the forefront of cloud adoption in CIs [11, 21, 25]. Especially in concerns of network simulations, highly flexible computing resources are needed. For example, renewable energy output is less predictable than conventional energy sources and thus demands for a flexible IT infrastructure [23]. Further examples for migrations to cloud computing environments are public sector institutions [7, 17, 21, 23] that use cloud services inter alia to implement e-government services or replace internal IT. The transport sector [2, 8, 21] adapts clouds for centralized service provisioning and traffic management via web-based interfaces. In the financial industry, where IT costs are estimated to represent around 15-20% of the banks' overall administrative expenses [16], the adoption of cloud solutions is promising. However, financial institutions are subject to strict regulations, e.g. regarding risk management and security. Thus, IT capacities for certain services have to be provided in-house in the medium and long term.

The major adopters of cloud solutions were found to be the energy as well as the finance/insurance sector with a total of four cases of application each, followed by energy/water (3), transport/traffic (3), water (2), telecommunications (1) and food (1). The finding that the energy sector is leading in cloud adoption corresponds to the estimation of expert no. 4 as well as the current study on cloud usage in Germany of KPMG [27]. Further, the expert states that the adoption is expanding but still "hampered by individual requirements of some organizations and sectors", e.g. the localization of services. However, as the majority of CIs identified was attributed to energy-related sectors (44) followed by information and telecommunication (14) and finance and insurance (5), the comparability is partially limited. The energy-related sectors consist to a large extent of municipal utilities, which only publish little information. Still, the relation of four out of five identified CIs from the finance/insurance sector that have adopted cloud solutions can be interpreted as high.

3.6 Risks

As outlined before, the risks resulting from a deployment of CI services and functionalities in cloud environments heavily depend on the selected cloud service and deployment model as well as the targeted business systems, processes and functions [13]. For example, in SaaS models, the security requirements and threats focus on the application level, whereas in PaaS and IaaS services virtualization aspects are rather critical [23]. Regarding the deployment models, outsourcing to public, community or hybrid clouds results in a loss of control and a dependency on the respective providers, in contrast to private solutions [18]. Thus, it is outside the scope of this article to provide a comprehensive overview of risks associated with cloud solutions. The latter can be found in control frameworks and standards like the ISO 27000 series or the CSA Cloud Controls Matrix. Further, Paudel et al. (2014) provide a list of security issues related to clouds [19]. The risk focus of CIs is put on IT security, privacy and resilience issues rather than on strategic or financial aspects, especially since CIs underlie stricter requirements [3]. Many risks result from common threats related to network and internet technology, and more rigorous precautions are needed when CI services are exposed in a cloud [22]. For CIs, the security and resilience risks as well as requirements associated to cloud usage are of central importance [2, 8, 18, 23]. For example, Mackay et al. (2015) provide an overview of CI requirements related to cloud usage and emphasize the importance of data security and integrity as well as availability. In this context, a further crucial point is the compliance with the various legal regulations that CIs underlie [22]. Thus, especially cloud-specific risks related to multi-tenancy, virtualization and the pooling of resources need to be evaluated in detail by CIs [8, 21]. At the same time, not all cloud-specific risks have a direct impact on the health, safety, security or economic well-being of citizens, for example a vendor lock-in [21]. Hence, the perspective of CIs on cloud risks differs compared to other enterprises. Another vitally important aspect, that was also expressed in all interviews, concerns the applicable privacy laws and jurisdiction over the data, as the location of data in clouds is often unknown [18].

There are also risks that arise regardless of the specific service model. This is the case with network dependencies and the consequent propagation of risks that result from the interaction of multiple CIs and clouds [7]. Further, cloud environments that run CI services become a more attractive target for attackers [8, 18]. Therefore, CIs need transparency over logical and physical dependencies of CIs and cloud providers [21]. Hence, CIs should conduct a detailed risk assessment and vulnerability analysis, which is followed by an effective risk monitoring and management [18].

4 Research Agenda

The analysis of the status quo of cloud computing in CIs revealed several research gaps, which mainly concern technical (T), jurisdictional (J), organizational (O) and contractual (C) issues. Therefore, Table 3 only illustrates an extract of potential topics for future research. In this context, it is possible to put the research focus on other areas, e.g. solely on technical IT security issues and related risks.

Table 3. Research Agenda for Cloud Usage in Critical Infrastructures

Gap	*No., Research Proposition/Issue [Reference] (Expert) {Practical Analysis}*
T	1. Analysis of interdependency risks of cloud and CI providers [7, 18, 21, 28] (1-4)
	2. Hybrid cloud frameworks and environments for CIs [7, 22, 23, 25] (2) {P}
	3. Secure data transfer to third parties over external networks [19, 22] (1, 2)
	4. Access controls that meet the security requirements of CIs [5, 8, 11, 19, 22, 23] (4)
	5. Deployment of critical business functions in (public) clouds [7, 22, 24] (4) {P}
J	1. Analysis of cloud-related requirements of national CI laws [13, 18, 21, 22] (1, 4)
	2. Legally compliant implementation of CI requirements at the provider [8, 29] (1, 2)
	3. Analysis of privacy issues particularly relevant for CIs [5, 8, 11, 18, 23] (1-4)
	4. Open security standards for cloud migration and deployment in CIs [4, 9, 19] (2)
	5. Legal transparency enforcement regarding data location and security [4, 8, 29] (2)
O	1. Development of flexible cloud risk management solutions for CIs [2, 11, 13, 18]
	2. Investigation of trust relationships between entities [5, 7, 8, 11, 19, 22] (1, 3)
	3. Cloud integration of security incidents reporting to authorities [5, 13, 18, 21] (2, 4)
	4. CI-relevant risk models for individual sectors and cloud deployments [2, 4, 18, 21]
C	1. Investigation of contractual relationships between CIs and cloud service providers, i.e. enhancement of SLAs or smart contract solutions [5, 8, 11, 22, 26, 29] (2, 4)
	2. Continuous assurance of legal security requirements [4, 5, 8, 11, 19, 20, 22] (1, 4)

The literature analysis unveiled that depending on the service and deployment model selected, the respective risks vary [13, 23, 25] (O4). In this context, hybrid cloud solutions combine the benefits of public and private clouds (T2). Although the risks for CI operators cannot completely be eliminated, they can at least be minimized. Thus, there is a need for a flexible risk management that allows for the consideration of individual circumstances and national legislations, especially for large and globally operating CIs (J1, O1). The adoption of cloud solutions by CIs results in a complex and opaque network of various actors and parties. Given the dependencies between cloud services and other actors risk assessments are often difficult [28]. Hence, the understanding of the involved actors, risks and dependencies is vital for sustainable business relationships of CIs and their cloud service providers to address the resulting technical and legal requirements [8] (T1). A further research topic is the area of trust, as trust is a central element in the outsourcing relationship between CIs and cloud providers [5, 8, 11, 19, 22]. This comes especially true when considering large and opaque public cloud services that rely on other cloud providers unknown to the direct contractual partner, i.e. the CI. Thus, there is a need to investigate such three-part trust relations and their impact on outsourcings (O2). In this context, the contractual configuration between the stakeholders in terms of SLAs is of further decisive importance in order to meet the specific demands of CIs [8, 22, 29] (C1). As SLAs are often predefined by cloud providers, the specific requirements of CIs and responsibilities of the parties need to be defined [7, 11, 23, 25]. In addition, there is a need for continuous assurance that the determined agreements are enforced, e.g. by appropriate certification methods [4, 8] (C2). The interplay of the actors with the corresponding research propositions and issues of Table 3 are displayed in Figure 1.

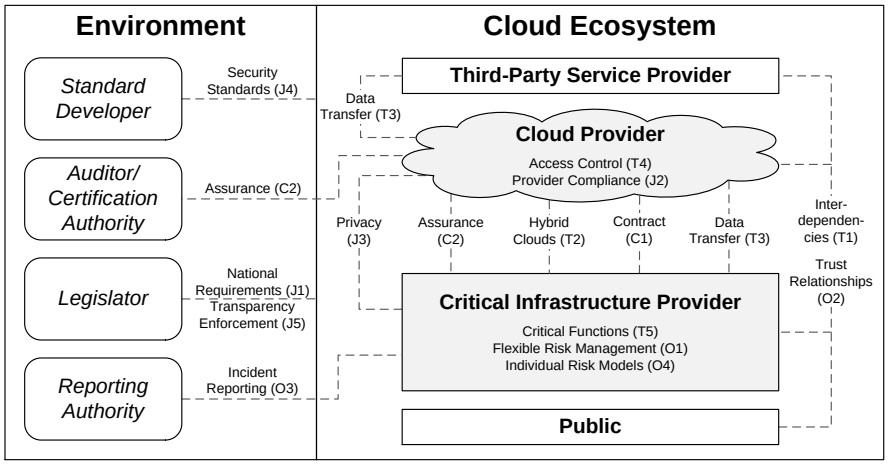

Figure 1. Open Issues and Research Propositions for Cloud Adoption in CIs [30]

5 Conclusion

The analyses revealed that cloud computing is only used in partial areas of critical infrastructures. Risks related to data security lead to a rather restrained attitude of many organizations. Yet, due to the fact that outsourcing into a cloud is advantageous, an increasing number of CIs decide to adopt cloud solutions for 'non-critical' business functions. Thus, future research on cloud solutions for core functions of CIs, such as industrial control systems [24], is necessary. Among the cloud services used by CIs private clouds for basic infrastructure services are considered frequently. Further, the use of services hosted in public clouds expands, especially SaaS. However, regulations and unclear legislations are obstacles for the adoption of cloud solutions by CIs, specifically in sectors with strict requirements for data privacy and security, such as finance or health. Thus, the assurance over actions and security measurements of the cloud provider and a minimization of dependencies are crucial. In summary, it can be stated that despite the increasing demand various aspects have to be considered and clarified, such as risk management issues. In this context, the results of the analysis of the current status quo of cloud computing in CIs are helpful for CIs and cloud providers alike to sustainably decide for or against cloud solutions.

However, the study has to be viewed under the light of some limitations. First, the practical analysis does not reflect the overall ratio of German CIs. Further, as we had to rely on publicly available information, the generalizability of the results is limited. As expert no. 4 stated that the risks associated to the disclosure of internal information on the IT landscape and outsourcings induce CIs to consciously withhold such information, we assume that the actual user numbers are significantly higher. In addition, it was not always clear whether the CIs use a classic IT outsourcing model or a cloud, and in case if, which kinds of cloud services were used particularly. Further, the results of the expert interviews might be biased by the sector affiliation of the respondents. Likewise, further interviews covering all CI sectors are desirable.

Acknowledgements

The authors thank the project members, especially Ms. Anne Christin Münning, Ms. Maria Borgmann, Mr. Niclas Bruhne, Mr. Heiko Halstenberg and Mr. Jonas Brinker for their valuable help and support during the research process. Furthermore, the authors thank Ms. Imhorst as well as the reviewers for their constructive feedback.

References

1. Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2016. (2016)
2. Hecht, T., Smith, P., Schöller, M.: Critical Services in the Cloud: Understanding Security and Resilience Risks. In: 6th International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 131–137. Barcelona, Spain (2014)
3. Bless, R., Hutchison, D., Schöller, M., Smith, P., Tauber, M.: SECCRIT: Secure Cloud Computing for High Assurance Services. ERCIM NEWS. 95, 40–41 (2013)
4. Wagner, C., Hudic, A., Maksuti, S., Tauber, M., Pallas, F.: Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud. In: 3rd International Conference on Future Internet of Things and Cloud. Rome, Italy (2015)
5. Hudic, A., Hecht, T., Tauber, M., Mauthe, A., Santiago Cáceres, E.: Towards Continuous Cloud Service Assurance for Critical Infrastructure IT. In: 2nd International Conference on Future Internet of Things and Cloud, pp. 175–182. Barcelona, Spain (2014)
6. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A.: Cloud Computing - The Business Perspective. Decision Support Systems. 51, 176–189 (2011)
7. Diez, O., Silva, A.: Reliability Issues Related to the Usage of Cloud Computing in Critical Infrastructures. In: Bérenguer, C., Grall, A., Guedes Soares, C. (eds.) Advances in Safety, Reliability and Risk Management: ESREL 2011. Troyes, France (2011)
8. Schöller, M., Bless, R., Pallas, F., Horneber, J., Smith, P.: An Architectural Model for Deploying Critical Infrastructure Services in the Cloud. In: IEEE International Conference on Cloud Computing Technology and Science, pp. 458–465. Bristol, UK (2013)
9. Paudel, S., Tauber, M., Brandic, I.: Security Standards Taxonomy for Cloud Applications in Critical Infrastructure IT. In: 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 645–646. London, UK (2013)
10. Rudolph, M., Schwarz, R., Jung, C.: Security Policy Specification Templates for Critical Infrastructure Services in the Cloud. In: 9th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 61–66. London, UK (2014)
11. Younis, Y.A., Merabti, M., Kifayat, K.: Secure Cloud Computing for Critical Infrastructure: A Survey. Liverpool John Moores University, Technical Report 599-610 (2013)
12. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems. 21, 11–25 (2001)
13. Adelmeyer, M., Petrick, C., Teuteberg, F.: IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes. HMD Praxis der Wirtschaftsinformatik. 54, 111–123 (2017)
14. Brocke, J. vom, Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the Giant: on the Importance of Rigour in Documenting the Literature

Search Process. In: 17th European Conference on Information Systems (ECIS), pp. 2206–2217. Verona, Italy (2009)
15. Gläser, J., Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse. Springer VS Verlag für Sozialwissenschaften, Wiesbaden (2010)
16. Lampe, U., Müller, A., Wenge, O., Schaarschmidt, R.: On the Relevance of Security Risks for Cloud Adoption in the Financial Industry. In: 19th Americas Conference on Information Systems (AMCIS). Chicago, Illinois, USA (2013)
17. Anastacio, M.M.B., Blanco, J.A.R., Villalba, L.J.G, Al-Dahoud, A.: E-Government: Benefits, Risks and a Proposal to Assessment Including Cloud Computing and Critical Infrastructure. In: 6th International Conference on Information Technology (ICIT). Amman, Jordan (2013)
18. Chochliouros, I.P., Spiliopoulou, A.S., Stephanakis, I.M., Arvanitozisis, D.N., Sfakianakis, E., Belesioti, M., Georgiadou, E., Mitsopoulou, N.: Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also Focusing upon the Cloud Perspective. In: 16th International Conference on Engineering Applications of Neural Networks (INNS). Rhodes Island, Greece (2015)
19. Paudel, S., Tauber, M., Wagner, C., Hudic, A., Ng, W.-K.: Categorization of Standards, Guidelines and Tools for Secure System Design for Critical Infrastructure IT in the Cloud. In: 6th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 956–963. Singapore, Singapore (2014)
20. Tauber, M., Wagner, C., Pallas, F.: Sicherheit und rechtliche Herausforderungen in Bezug auf Cloud Computing und Kritische Infrastruktur-IT. e & i Elektrotechnik und Informationstechnik. 131, 33–36 (2014)
21. Dekker, M.A.C.: Critical Cloud Computing. Technical Report, European Network and Information Security Agency (ENISA) (2012)
22. Mackay, M., Baker, T., Al-Yasiri, A.: Security-oriented Cloud Computing Platform for Critical Infrastructures. Computer Law & Security Review. 28, 679–686 (2012)
23. MacDermott, A., Shi, Q., Merabti, M., Kifayat, K.: Hosting Critical Infrastructure Services in the Cloud Environment Considerations. International Journal of Critical Infrastructures. 11, 365–381 (2015)
24. Piggin, R.: Are Industrial Control Systems Ready for the Cloud? International Journal of Critical Infrastructure Protection. 9, 38-40 (2015)
25. MacDermott, A., Shi, Q., Merabti, M., Kifayat, K.: Protecting Critical Infrastructure Services in the Cloud Environment. In: 12th European Conference on Information Warfare and Security (ECIW), pp. 336–343. Jyväskylä, Finland (2013)
26. Niekerk, B. van, Jacobs, P.: Cloud-based Security Mechanisms for Critical Information Infrastructure Protection. In: International Conference on Adaptive Science and Technology (ICAST). Pretoria, South Africa (2013)
27. KPMG: Cloud-Monitor 2017. Technical Report, KPMG, Bitkom (2017)
28. Keller, R.: Analyse von Risikomanagementstrategien in Cloudnetzwerken – Was tun bei verknüpften, voneinander abhängigen Cloud Services? HMD Praxis der Wirtschaftsinformatik. 53, 674–687 (2016)
29. Florian, M., Paudel, S., Tauber, M.: Trustworthy Evidence Gathering Mechanism for Multilayer Cloud Compliance. In: 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 529–530. London, UK (2013)
30. Floerecke, S., Lehner, F.: Cloud Computing Ecosystem Model: Refinement and Evaluation. In: 24th European Conference on Information Systems (ECIS). İstanbul, Turkey (2016)