SECCRIT Online Survey on Cloud Security for Critical Infrastructure IT

1 Introduction

The SECCRIT (SEcure Cloud computing for CRitical infrastructure IT) project is a multidisciplinary research project with the mission to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and highly assured cloud computing environment for critical infrastructure IT. The project is a collaborative EU-funded research project in the 7th Framework Programme (FP7-SEC-2012-1).

1.1 Motivation of the study

Fraunhofer IESE started this survey to elicit cloud security needs for developing methodologies and tools for improving the security in cloud infrastructures within the SECCRIT project. Therefore, an online questionnaire was created.

1.2 Mode of participation and result evaluation

Participation in the survey was voluntary. Moreover, if participants felt unable or unwilling to answer individual questions, they were allowed to leave the corresponding answers blank.

All answers of the participants are handled confidentially. There was the option to participate anonymously. Individual answers are not disclosed to any third party outside the SECCRIT project team at Fraunhofer IESE, and they will be used only for scoping the SECCRIT research agenda. Only aggregated results will be evaluated and published.

1.3 Participants

The survey was only offered to members of the SECCRIT User and Advisory Board. The User and Advisory board consisted at the time of the invitation to the online survey of representatives

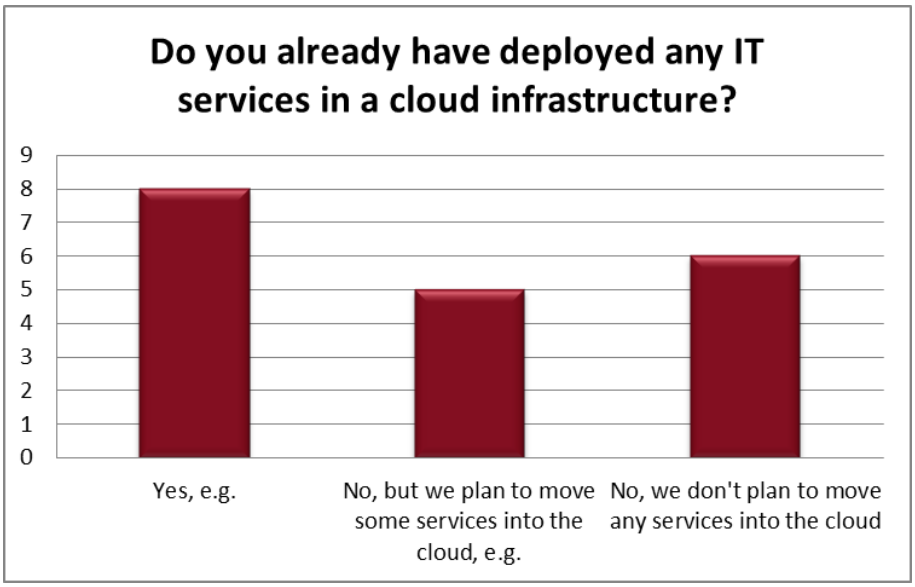
from 46 companies that are settled in the domain of critical infrastructure or that are cloud providers. In total, 60 persons from those companies were asked for participation.

2 Results

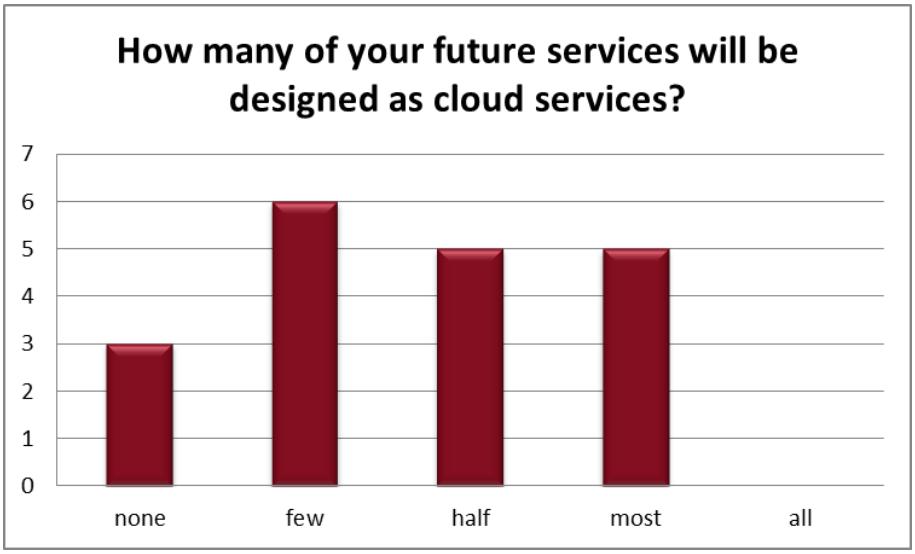
From 60 invited participants representing 46 companies, 19 started the survey and partially answered the questionnaire. Fifteen participants completely finished the questionnaire. We do not claim that the results are statistically significant due to the limited number of participants and the bias of the participant selection. However, the results can reveal trends in the domain of cloud computing regarding IT security.

2.1 Cloud Usage

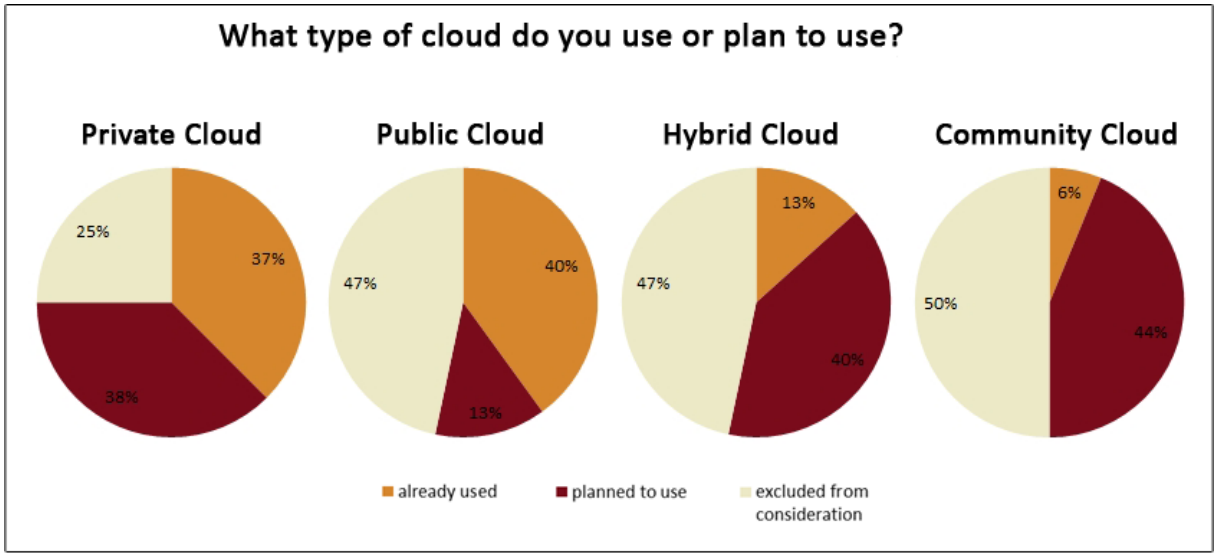
The first set of questions investigated the current and planned usage of cloud infrastructures in general and for the specific purpose of hosting critical infrastructures in particular.

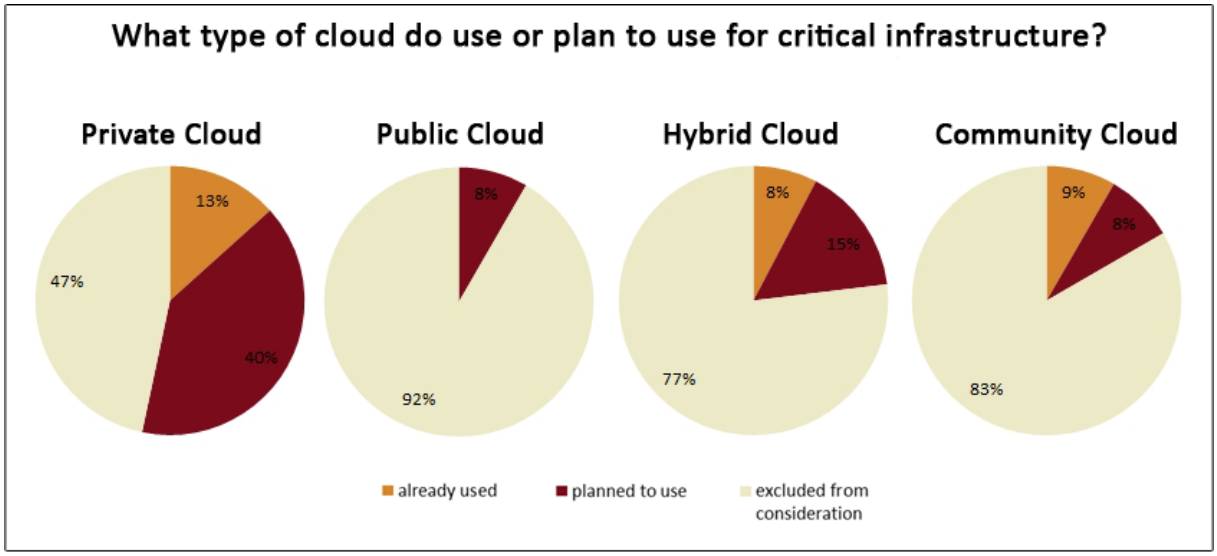


Those participants considering cloud deployment were asked to provide examples of intended cloud services. Eight participants already deployed services in cloud infrastructures, such as data management systems, business process management, email and calendars services, CRM systems, MS Exchange, and GitHub. Five participants currently plan to move services into the cloud, such as Smart Services. Moreover, some participants stated to use cloud infrastructures such as Google Docs and Amazon S3.



Participants stated that their organisations plan to employ cloud solutions to a varying degree in the future. Accordingly, different types of cloud infrastructures were considered by the participants' organisations. A private cloud is exclusively used by one organisation, while a public cloud is open to any organisation. A hybrid cloud has public as well as private partitions. A community cloud only hosts services of a closed user group.

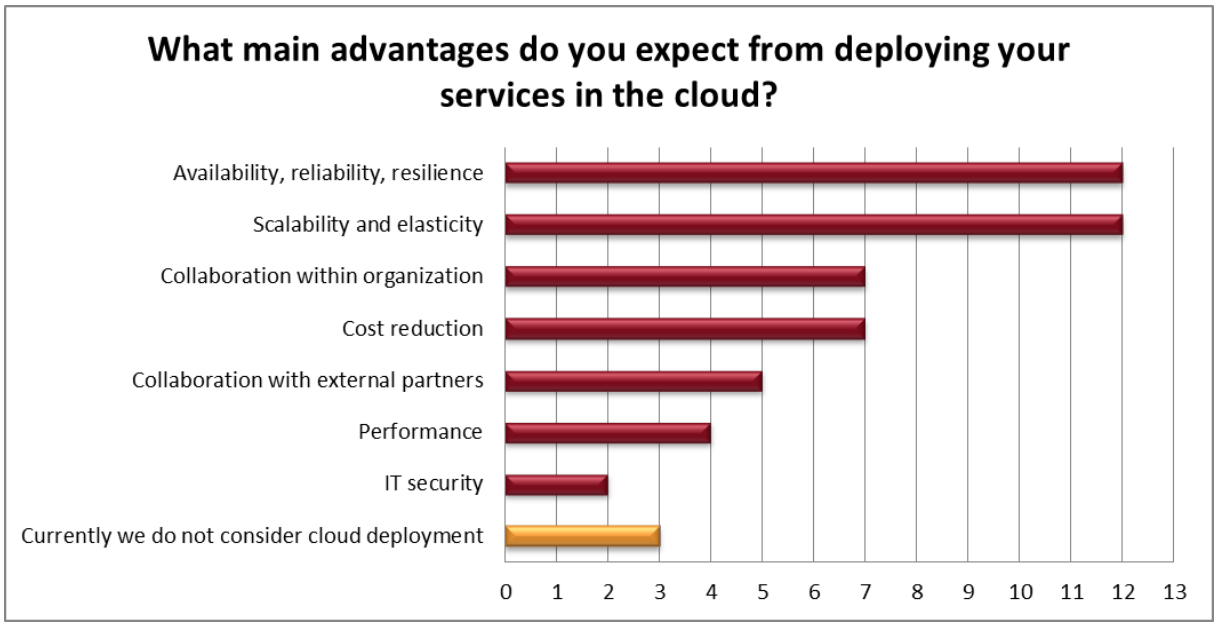




The survey indicates that the participants still have strong reservations using non-private cloud infrastructures. Those reservations increase when deploying critical infrastructure services. Private clouds seem to be an acceptable solution within the SECCRIT User and Advisory Board, even for running critical infrastructure services.

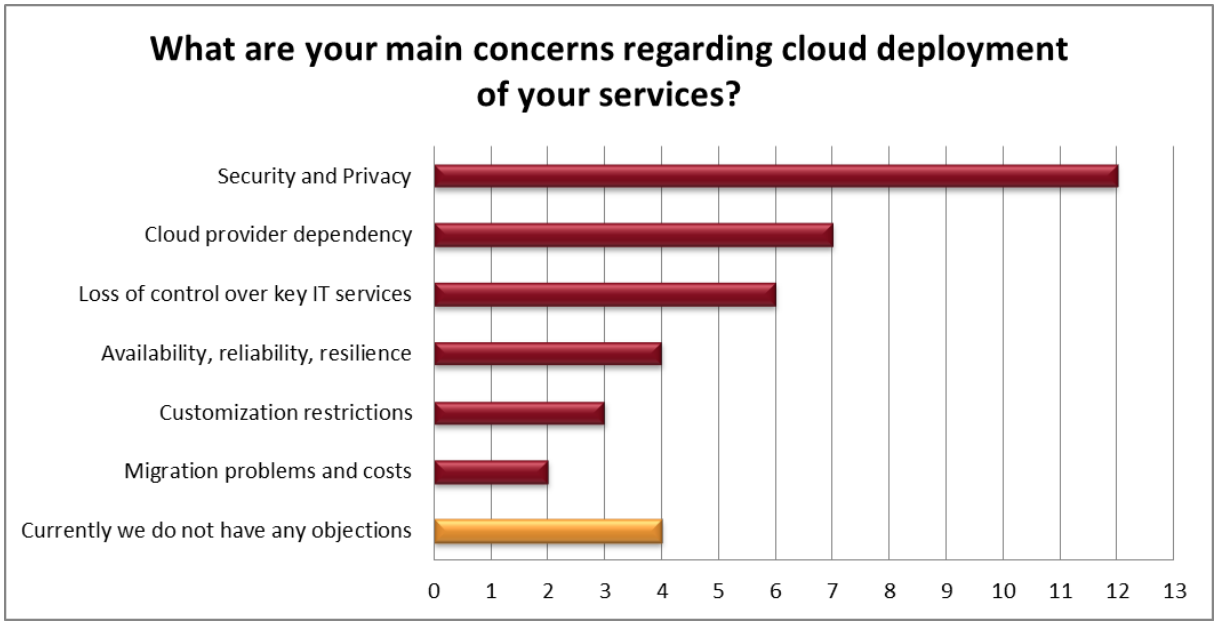
2.2 Advantages and Concerns

In the second set of questions, we asked the participants to vote for the main advantages and concerns for their organisations of deploying services in the cloud. Multiple responses were allowed.

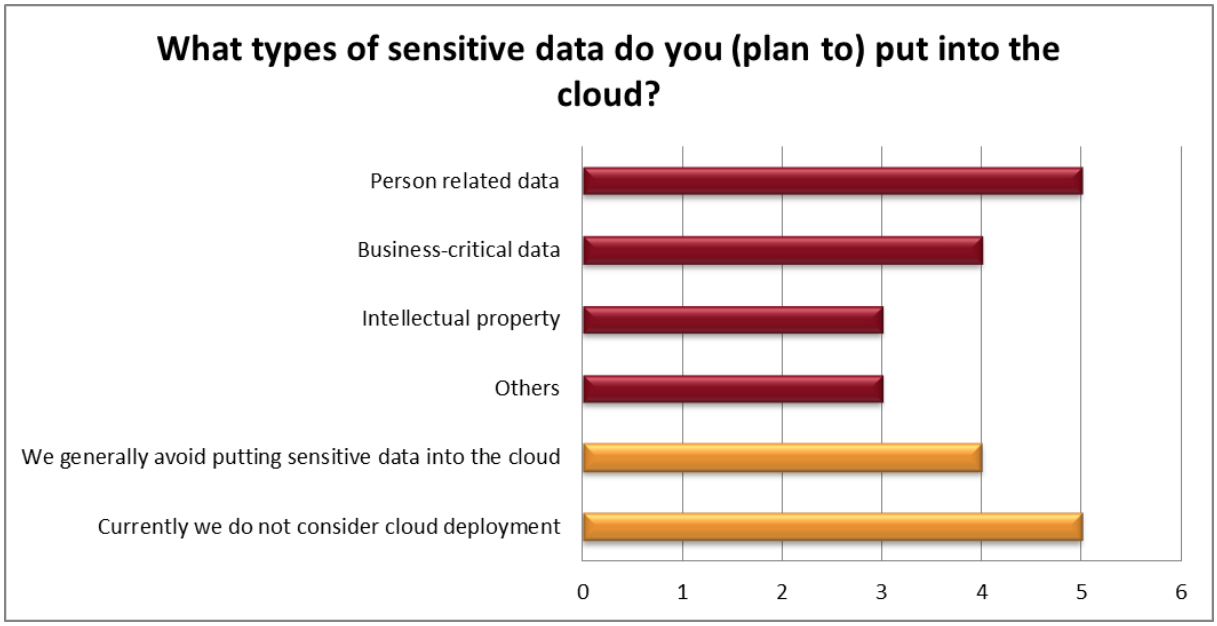


Besides the economic advantages of deploying services in the cloud, such as cost reduction, scalability and elasticity, especially safety-related advantages, such as availability, reliability and resilience, are expected. In addition, collaboration reasons are an inducement for moving services into the cloud.

Interestingly, some respondents expected even advantages with respect to IT security. This is remarkable because cloud solutions generally raise security concerns, as the answers to the next survey questions confirm.



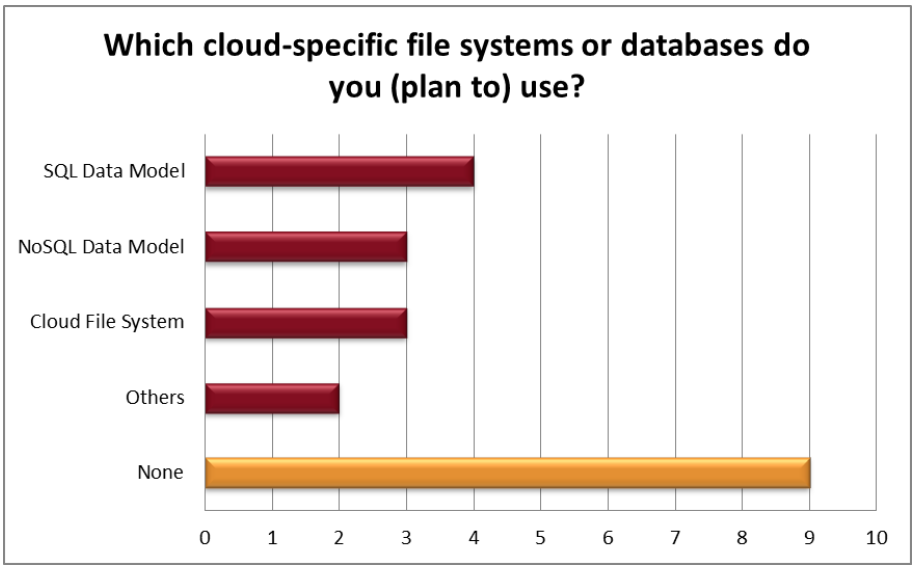
The majority considered security and privacy as their main concern regarding service deployment in cloud infrastructures. Other critical issues seem to be the dependence of cloud providers and loss of control over key IT systems and the infrastructure itself.



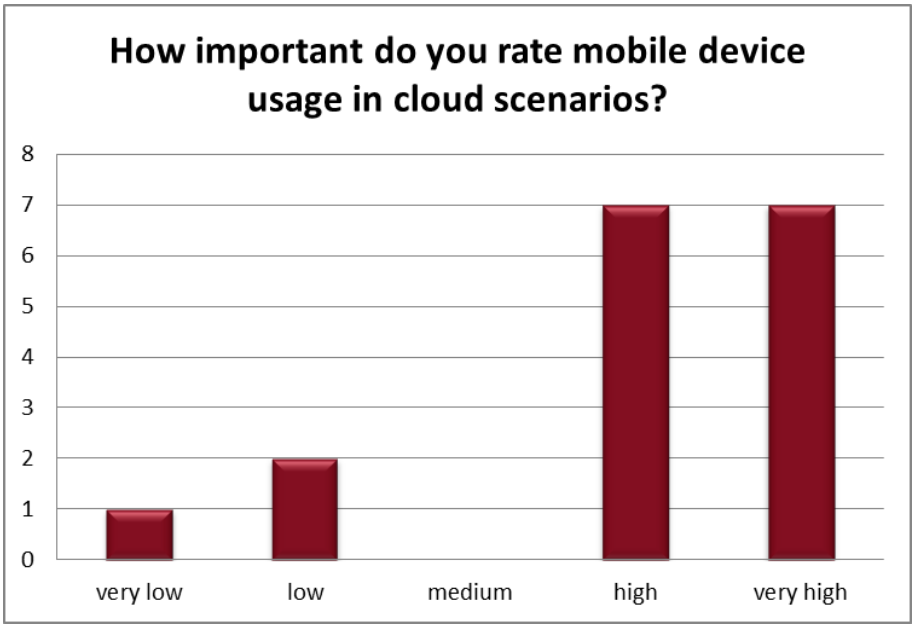
About half of the respondents still have strong reservations putting sensitive and potentially business critical data into the cloud. The remaining answers of those participants who actually (plan to) put critical information into the cloud cover all types of sensitive data.

2.3 Specific features

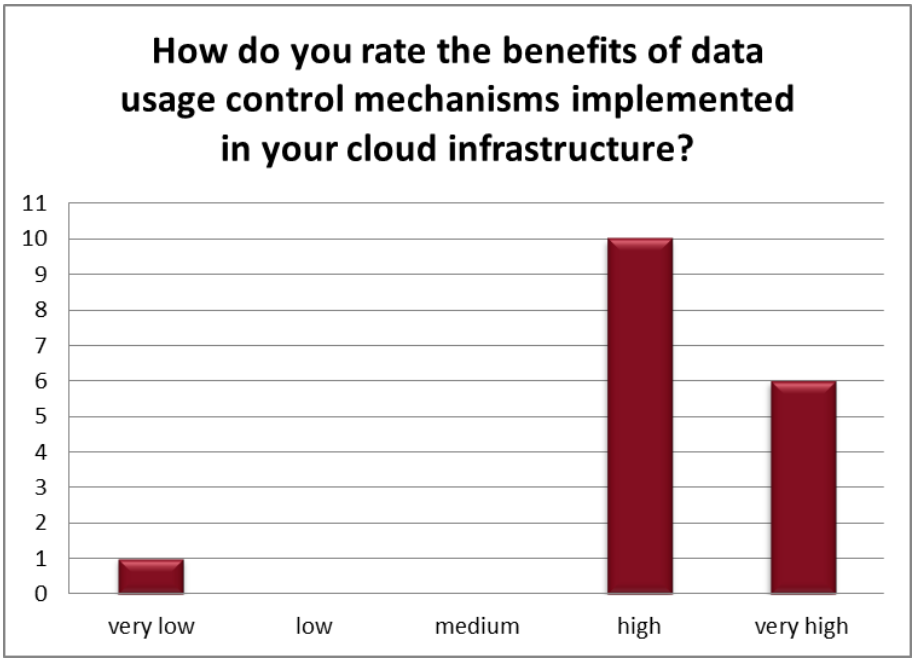
The third set of questions covered specific features that may be demanded in cloud solutions.



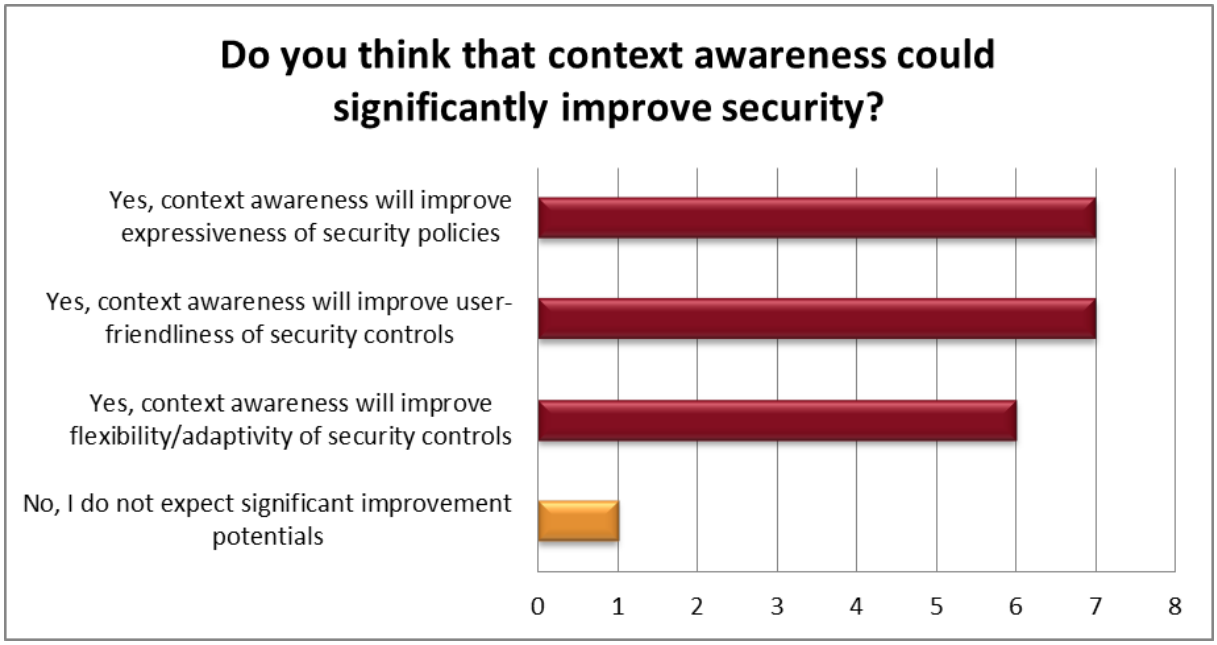
About half of the participants in the survey stated that they use or plan to use cloud-specific file systems or databases. Those are demanded for exploit the full potential of cloud infrastructures, such as elasticity, scalability, or performance. Interestingly, nine respondents do not plan to use cloud-specific file systems or databases. Further investigations are necessary to clarify whether these participants are not yet aware of the potential advantages of such solutions or whether they really do not need any of those features.



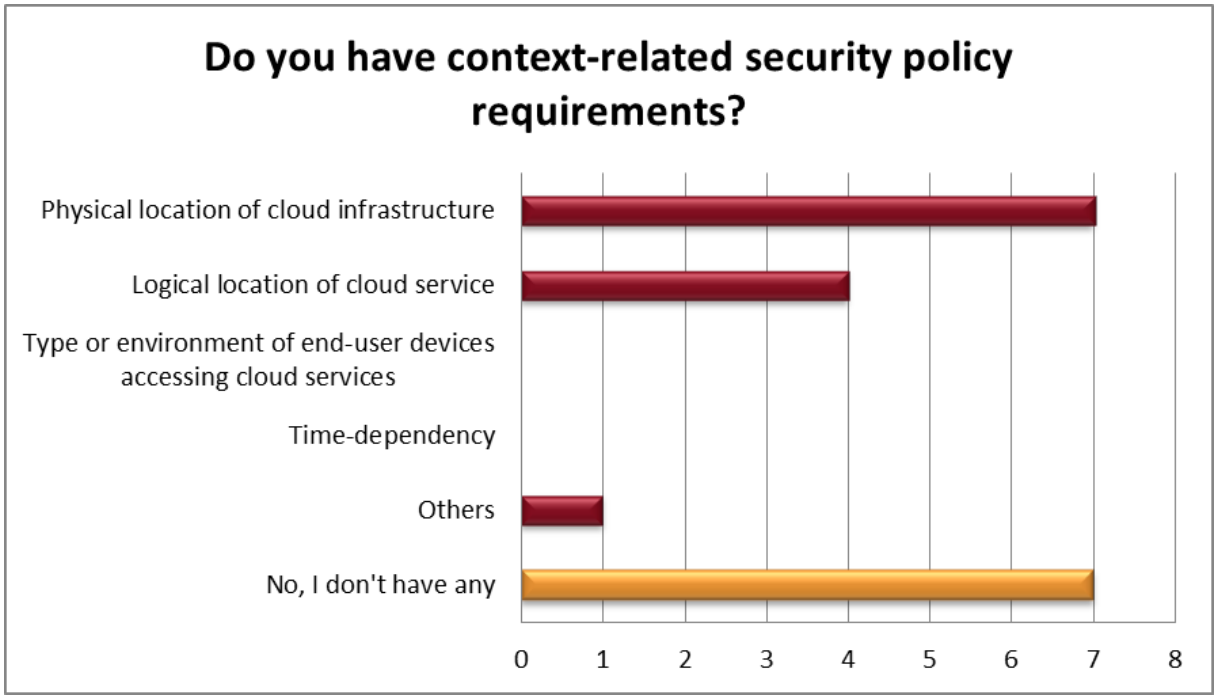
The majority of respondents believed that mobile devices are an important part of cloud solutions. Therefore, security concepts in cloud infrastructures should reflect the peculiarities of such mobile devices.



Data usage control is a generalisation of access control. It enables the control over data usage after initial access on data has been granted to entities other than the data owner. Almost all respondents saw a significant need for data usage control mechanisms in their cloud infrastructures.



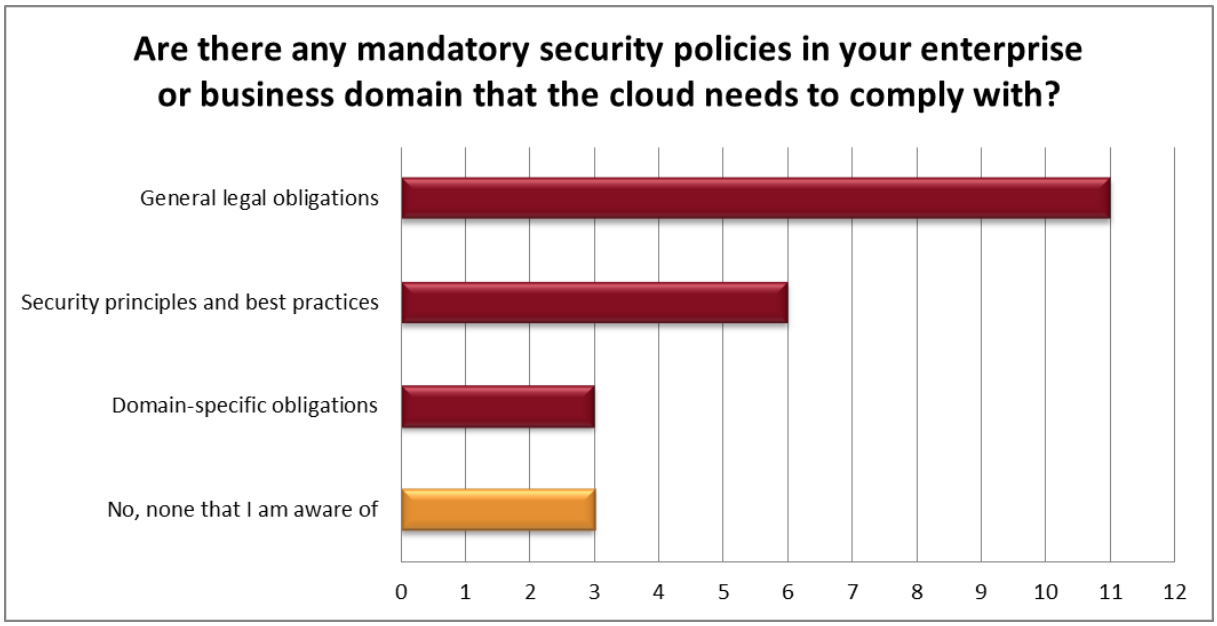
A system is context-aware if it is able to adapt to the system's or its user's current operational scenario. For example, a mobile device may detect that its user is currently in a confidential business meeting and may automatically disable the voice recording function. Almost all respondents agreed that context awareness has a positive impact on IT security.



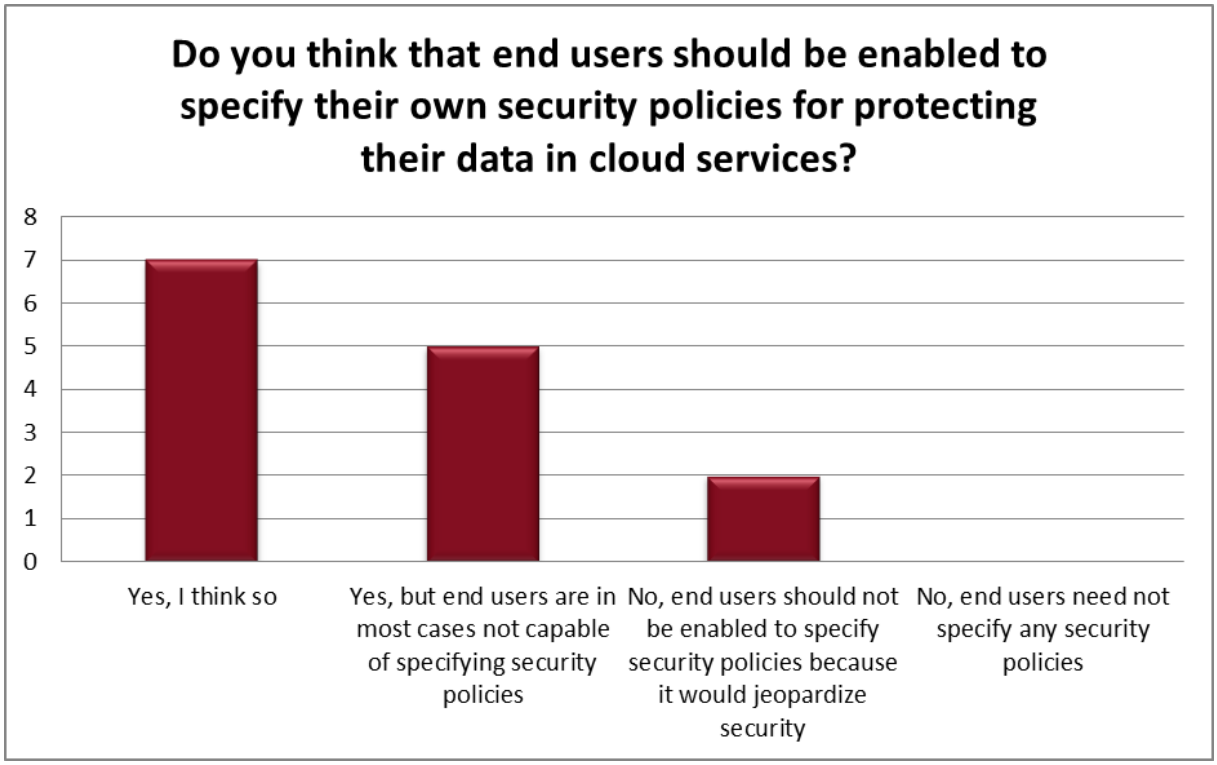
Some of the participants seem to have a demand for context-related security policies in cloud infrastructures, such as controlling the physical location of cloud infrastructures and the logical location of services within the cloud infrastructure.

2.4 Security Policies for the Cloud

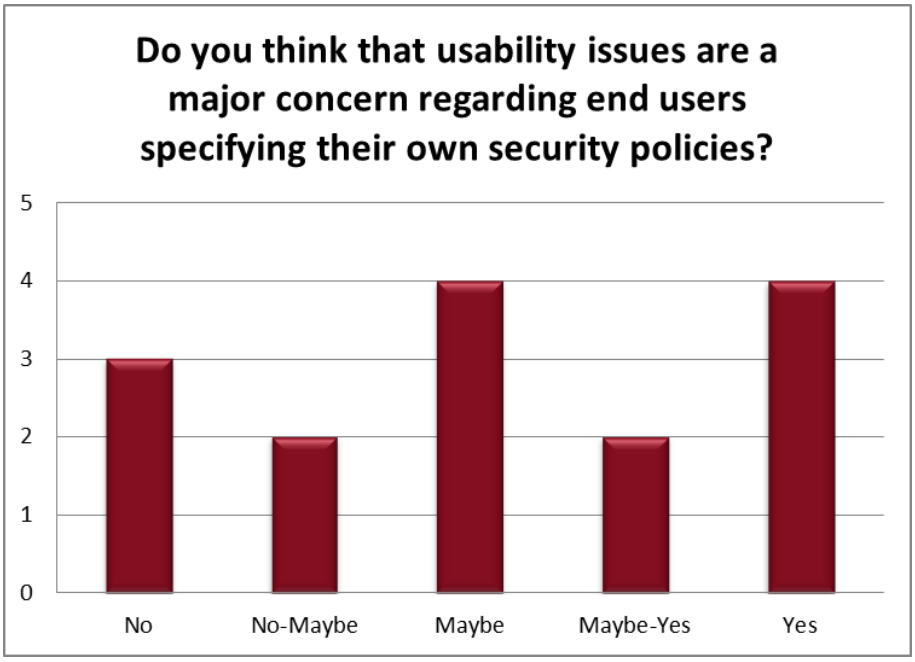
The last set of questions covered the role of security policies in cloud infrastructures.



Participating organisations revealed that they mainly apply security policies on the cloud to comply with legal obligations. Legal metrology was stated as an example for security policy application. Moreover, security principles, best practices, and domain-specific obligations such as consumer protection laws are enforced in cloud infrastructures.

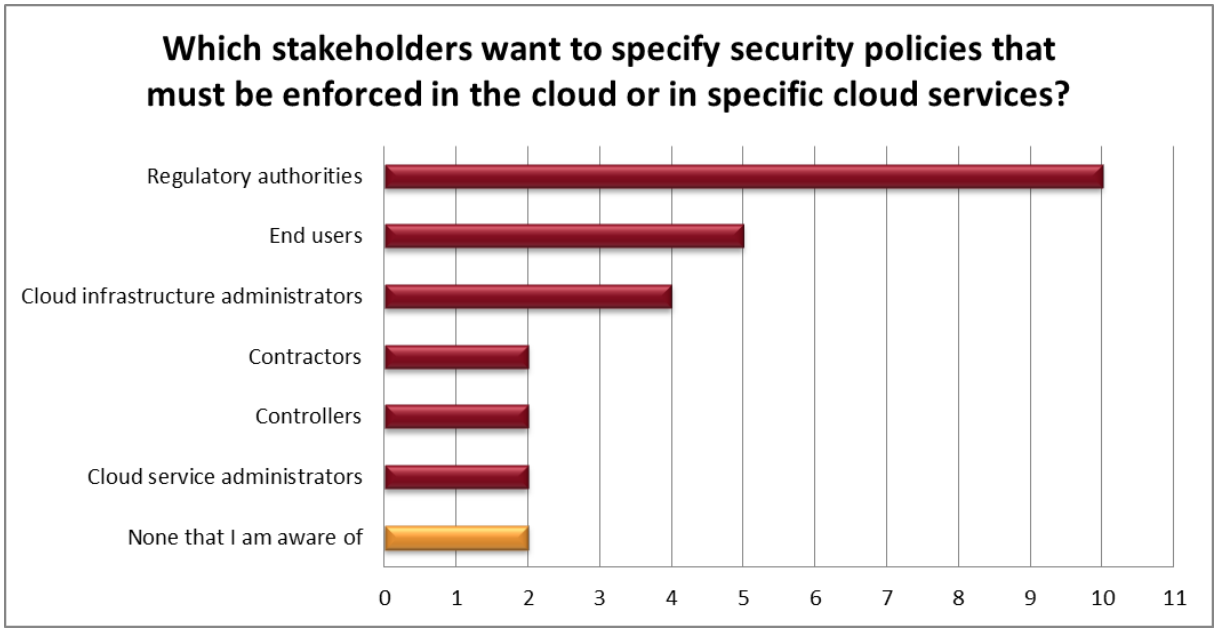


Most participants stated that in their opinion, end users should be enabled to specify security policies on their own for protecting their individual data in cloud services. However, some respondents doubt that end users are capable of specifying correct security policies, or they suspect that such a functionality of cloud infrastructures would jeopardise security. Not a single respondent denied the need for user-specified security policies for protecting data in cloud services.



The question whether usability issues are a major concern regarding the specification of security policies by end users yielded an inconclusive result. Further investigations must clarify whether

enhanced usability of policy specification tools can improve the ability of end users to specify their own security policies, user acceptance, and the willingness of cloud and service providers to provide such policy specification mechanisms.



Different stakeholders have an interest in applying security policies on the cloud or on specific cloud services. Participants named regulatory authorities and end users as the main policy contributors.

3 Conclusion

This survey revealed trends in the domain of cloud computing when deploying critical infrastructure services. In general, there is a strong trend towards cloud computing. Thus, many future services are planned as cloud services. To this end, the use of private clouds is preferred. This is especially the case when employing critical infrastructure services. Strong objections prevail over non-private clouds. Participants stated cost reduction, scalability, elasticity and especially availability, reliability, and resilience as the main advantages of cloud infrastructures for their organisations. The majority of the respondents claimed security and privacy as well as loss of control over key IT systems and the infrastructure itself as their main concerns regarding service deployment in cloud infrastructures.

The survey confirmed the need for usage control in cloud infrastructures. Especially context-aware security policies are requested. Most participants see an important role for mobile devices in cloud infrastructures. There is a need for end users to specify security policies, but doubts arose whether they are capable of providing correct policy specifications that do not jeopardise security.

The results of this survey reflect only trends due to the limited number of participants and the bias of the participant selection. For achieving statistically significant results, the survey must be forwarded to a broader and more representative community.

4 Contact

This survey was carried out by Fraunhofer IESE in Kaiserslautern, Germany in the context of the SECCRIT project. If you have any further questions concerning the questionnaire, please contact Manuel Rudolph or Reinhard Schwarz at Fraunhofer IESE.

Manuel Rudolph M.Sc., Fraunhofer IESE
Information Systems Quality Assurance (ISQ)
Fraunhofer-Platz 1, 67663 Kaiserslautern, Germany
Phone/Fax: +49 631 6800 2289 / +49 631 6800 92289
manuel.rudolph@iese.fraunhofer.de
http://www.iese.fraunhofer.de

Dr. Reinhard Schwarz, Fraunhofer IESE
Information Systems Quality Assurance (ISQ)
Fraunhofer-Platz 1, 67663 Kaiserslautern, Germany
Phone/Fax: +49 631 6800 1204 / +49 631 6800 91204
reinhard.schwarz@iese.fraunhofer.de
http://www.iese.fraunhofer.de