Making secret sharing based cloud storage usable

Erik Framner and Simone Fischer-Hübner
Department of Mathematics and Computer Science, Karlstads Universitet, Karlstad, Sweden

Thomas Lorünser
Austrian Institute of Technology Department of Safety and Security, Wien, Austria

Ala Sarah Alaqra
Department of Mathematics and Computer Science, Karlstads Universitet, Karlstad, Sweden, and

John Sören Pettersson
Department of Information Systems, Karlstads Universitet, Karlstad, Sweden

Received 20 January 2019
Revised 28 June 2019
Accepted 29 June 2019

Abstract

Purpose – The purpose of this paper is to develop a usable configuration management for Archistar, which utilizes secret sharing for redundantly storing data over multiple independent storage clouds in a secure and privacy-friendly manner. Selecting the optimal secret sharing parameters, cloud storage servers and other settings for securely storing the secret data shares, while meeting all of end user's requirements and other restrictions, is a complex task. In particular, complex trade-offs between different protection goals and legal privacy requirements need to be made.

Design/methodology/approach – A human-centered design approach with structured interviews and cognitive walkthroughs of user interface mockups with system administrators and other technically skilled users was used.

Findings – Even technically skilled users have difficulties to adequately select secret sharing parameters and other configuration settings for adequately securing the data to be outsourced.

Practical implications – Through these automatic settings, not only system administrators but also non-technical users will be able to easily derive suitable configurations.

Originality/value – The authors present novel human computer interaction (HCI) guidelines for a usable configuration management, which propose to automatically set configuration parameters and to solve trade-offs based on the type of data to be stored in the cloud. Through these automatic settings, not only system administrators but also non-technical users will be able to easily derive suitable configurations.

Keywords Privacy, Decision support systems, Usability, Security, Cloud computing, Secret sharing

Paper type Research paper

This work was supported by the EU H2020 project PRISMACLOUD, Grant Agreement No. 44962, the DRBD4Cloud project of the Eurostars Programme, FFG Grant Agreement No. 861332, and the Swedish SSF project SURPRISE.

Information & Computer Security
Vol. 27 No. 5, 2019
pp. 647-667
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-01-2019-0016

1. Introduction

Cloud storage has become a commodity technique, commonly used by companies for dynamically outsourcing their data storage onto third-party servers. Benefits include increased agility by self-service and pay-per-use potentially leading to decreased monetary costs, access to managed storage without having to use storage specialists as well as improved off-site disaster recovery. The benefits from the cloud can be essential, especially for smaller companies and businesses. They do not need any capital expenditure (capex) on in-house storage/computing resources and can carefully plan their operational expenditure (opex) on a pay-per-use basis. However, drawbacks are also evident and mainly stem from the risks associated with the outsourcing paradigm that cloud computing is building on. In particular, the risks perceived by users are the increased dependency upon third-parties, vendor lock-in and loss of data sovereignty, privacy and security risks as well as service-level agreements that do not allow contractual enforcement of storage availability. Moreover, in similarity to in-house storage, the physical location of cloud storage provider's (CSP's) data centers may be struck by catastrophic events such as fires, earthquakes, floods or acts of war, which may cause the stored data to be unavailable or even permanently lost. Although this will not be a real threat for major CSPs that have large enough infrastructure with built-in redundancy to mitigate them, it can be relevant risks for smaller local providers. Furthermore, a dearth of transparency about where data are and how data are being handled could be regarded as characteristics of insufficient user control, which in turn may discourage cloud storage adoption (Pearson, 2013). However, existing cloud offerings in the business domain have changed a lot in this respect and providers give users detailed information about storage locations of their data or even enable geo-restricted placements, which make the services more attractive for the industry.

Companies outsourcing their sensitive backup data require data confidentiality, compliance with data protection legislations as well as resilience in case of partial cloud failures. Privacy-friendly solutions are also relevant for IoT applications when large amount of captured sensitive (e.g. health) data is archived in the cloud.

The use of cryptography for securely storing data in the cloud is not straightforward, because of the requirements found in cloud environments. It is the increased agility and capability of dynamically sharing data with different stakeholders, which involve complex key management and performance issues that may arise, which often make the use of well-established cryptographic methods unsuitable (Yu *et al.*, 2010; Ren *et al.*, 2012). Hence, many of the advantages of cloud computing are lost if standard encryption is used in many application scenarios.

Within the scope of the EU *H2020* PRISMACLOUD[1] project, the Archistar storage system has been developed as a fresh approach to build secure distributed storage systems that mitigate some of the above-mentioned issues (Lorünser *et al.*, 2016). Following the multi-cloud paradigm for better security (AlZain *et al.*, 2012; Bessani *et al.*, 2011; Correia, 2014), storage systems based on Archistar securely disperse their data redundantly over multiple independent storage clouds, thus limiting the damage potential of each single storage provider and thus protecting the availability and confidentiality of the data. At its core, Archistar applies secret sharing as encoding technique to protect data. The idea of secret sharing was first presented by Shamir (1979) and is used for splitting secret data into shares (or "chunks") which are distributed among a group of N cloud servers. That is, each server is allocated a share of the secret data, and the secret data can only be reconstructed when sufficient number k with $k \leq N$ of shares are combined. With the use of secret sharing to create the split-up data, increased data confidentiality can be gained compared to other methods like

replication. However, traditional security assumptions – such as mathematical strength of encryption algorithms – are replaced with a non-collusion assumption between the involved storage providers, meaning that at least $N - k + 1$ storage providers are assumed to not collude for reconstructing the data without permission of the data owner.

Moreover, for $k < N$, the risk of data loss is also reduced, as it introduces additional redundancy and if data are stored at multiple geographical locations, with sufficient distance between them, then Archistar can even protect from larger local disaster and significantly improve business continuity.

However, Archistar also needs to be carefully configured for adequately addressing the end user's legal privacy and security requirements for data archiving in the cloud in compliance with the EU General Data Protection Regulation – GDPR (European Commission, 2016; or any contractual and/or budgetary restrictions. Moreover, trade-offs between different protection goals such as data secrecy and data availability and cost restrictions need to be made.

During our work in the development of the Archistar service (Happe *et al.*, 2017), we experienced that it was hard even for technically skilled end users, including system administrators, to select the optimal secret sharing parameters (such as the numbers k and N), algorithms and/or the location and characteristics of cloud storage servers for securely storing the data shares, while meeting all of end user's requirements and restrictions. In fact, we think the lack of understanding of human factors in the deployment and operation of multi-cloud (storage) systems with security based on non-collusion is a major inhibitor to the broader adoption of this technology, which is ideally suited to give people more freedom and flexibility in the usage of cloud storage.

The research reported in this paper, therefore, addresses the research challenge of *making the configuration of Archistar usable for technically skilled users, including system administrators while meeting privacy, security, trust and other organizational requirements.*

For addressing this research challenge, we followed a user-centered design approach for analyzing the end user's needs from the beginning and considering them for the design of usable solutions for Archistar's configuration management. We decided to focus first on system administrators and technically skilled users that could be qualified to be responsible for configuring Archistar within different organizations, who not only have higher technical expertise than most lay users that may use Archistar for private purposes but also have to take more complex organizational restrictions into consideration than in the private use case. Our approach involved interviews with those end user representatives, followed by two iterations of user interface (UI) mockup developments and end user evaluation studies for elaborating on the following research questions:

RQ1. What are the end user requirements and preferences for technically skilled users including system administrators in organizations for using Archistar for enabling a multi-cloud storage based on secret sharing in terms of privacy, security, trust or any other organizational restrictions?

RQ2. How do these requirements and preferences translate to suitable cloud provider selection and parameter configurations?

RQ3. How can users of such a multi-cloud storage system be assisted in the configuration process to select suitable combinations?

The remainder of this paper is structured as follows:

Section 2 provides background information about secret sharing schemes for Archistar and legal privacy aspects and requirements for Archistar, as well as protection trade-offs to be made with Archistar.

Section 3 presents our end user studies, starting with the structured interviews and their results, which we conducted for answering the *RQ1* in Section 3.1.

In Sections 3.2, we will then present the results from the two iterations of mockup developments and evaluations for answering *RQ2* and *RQ3*. Section 4 discusses our main UI guidelines for Archistar and, thus, also addresses *RQ3*. Section 5 will discuss related work, and the overall conclusions for our research study are presented in Section 6.

2. Background

2.1 Secret sharing schemes for Archistar

Secret sharing as already introduced in Section I builds upon the concept of secure data dispersal and may not only increase data confidentiality but could also be used to increase the availability of data (Loruenser *et al.*, 2015). For storage applications, it is important that encode/decode steps are computational efficient, and the size of the fragments is optimally small for the required security properties (Stangl *et al.*, 2018). Therefore, in storage applications, mainly computational secret sharing (CSS) as proposed by Krawczyk (1994) is used, which is very similar to erasure coding (Li, 2012) in terms of its fragment size and k-out-of-n decoding properties. In fact, CSS chunks not only are by a factor of $1/k$ shorter compared to perfectly secure secret sharing as proposed by Shamir but also provide confidentiality guarantees as long as no more than $k - 1$ clouds collude (Lorünser *et al.*, 2016). Moreover, although CSS is not perfectly secure, it still provides strong security guarantees and as Shamir's scheme can also be considered quantum-safe.

Archistar (Loruenser *et al.*, 2015) is a software framework designed to build multi-cloud storage networks leveraging CSS among others and its goal is essentially to provide a more secure and trustworthy virtual cloud storage service on top of less reliable and less trusted cloud storages. It offers two modes of operation, dependent if active or passive storage nodes are assumed (Loruenser *et al.*, 2015; Happe *et al.*, 2017), one targeted archiving/backup and the other at collaborative online storage. The technology is mature, straightforward to configure and manage. However, the selection of good parameters and cloud offerings is still up to the user. While this ensures the highest flexibility, it also burdens users with complex decisions compared to the selection of a single cloud storage offering.

Currently, suitable HCI concepts for simplifying this decision process are lacking for Archistar and for secret sharing-based secure multi-cloud storage applications in general, which motivates our work.

2.2 Legal aspects

2.2.1 The legal nature of secret sharing. As discussed above, a single secret chunk is, depending on the secret sharing protocol, either information theoretically or computationally secure against the reconstruction of the original data. If it is, however, combined with $k - 1$ other shares, then the data can be reconstructed. Splitting data into secret shares and storing them separately, therefore, fulfills the definition of *pseudonymisation* of Art. 4 (5) GDPR. As stated in this definition and in Recital 29 of the GDPR, pseudonymous data should still be considered as personal data. Hence, if European data controllers are outsourcing secret shares of personal data when using Archistar, then legal privacy provisions of the GDPR and other applicable privacy laws have to be met.

2.2.2 Legal privacy requirements. In particular, the following legal requirements of the GDPR are of importance when selecting cloud servers for storing personal data with Archistar.

First, pursuant to Article 28 GDPR, the outsourcing of personal data from the data controller to a cloud provider taking the role of a data processor needs to be governed by a contract, a so-called data processing agreement, between the controller and the processor. This agreement shall stipulate that personal data are only processed on documented instructions from the controller and that appropriate technical and organizational security measures are taken. This means that secret shares of personal data may only be transferred by the controller to those cloud storage providers, with whom the controller has such an agreement.

Moreover, when selecting cloud providers outside of Europe for storing secret shares the adequacy principle of Art. 45 GDPR has to be followed unless other legal grounds defined in Art. 46-49 GDPR (via for instance standard data protection clauses, binding corporate rules or explicit consent) allowing the data transfer apply. The adequacy principle requires that in principle, personal data may be transferred to a third country outside the EU only if the European Commission has decided that the third country, a territory or one or more specified sectors within that third country or the international organization in question ensures an adequate level of protection.

2.3 Trade-offs between goals

The protection goals security and privacy as well as cost requirements of an organization may to some extent be in a conflict with each other, for instance in regard to the choice of the parameters k out of N. In this section, we discuss the typical aspects to be considered in the configuration of a multi-cloud storage system on the basis of CSS encoding, which is the most relevant one for practical application.

- For a cost minimal solution, the number of spares ($N - k$) should be low (as more redundant servers increase the costs). Moreover, having a high N in general could also increase the cost on the administrative side which suggests having lower N in general for less administrative overhead.
- For availability in terms of disaster recovery, N should be higher than k to have redundancy in the system. The higher ($N - k$) is, the better the availability gets based on the *k-out-of-N* behavior of the system. However, with increasing k and also N, the number of nodes that will need to cooperate increases; this could also lower the performance of the system in terms of latency and throughput for data access. A more detailed discussion of configuration parameters to achieve certain availability can be found in Happe *et al.* (2017).
- For privacy protection, the threshold k should be high to minimize the risk of collusion and, thus, of data breaches. Moreover, $N - k$ should be low, to keep the overall number of parties low, that is, with increasing N, the number of potential adversaries increases. While for preventing data breaches, k should ideally be equal to N; privacy protection also requires protecting the availability of data, and thus, choosing a threshold $k < N$ is still recommended.

Moreover, the different protection goals may also translate into different requirements for the geographic server locations. In the previous section, we discussed legal privacy requirements for the server locations. For preventing data losses in terms of disasters, server locations should rather be distributed for minimizing the risks that different servers are hit

by the same natural disaster, while for providing high server up-time guarantees, the distance of the server locations from the end user should be minimized.

3. End user studies

For addressing *RQ1*, end-user requirements and preferences were elicited through structured interviews conducted during spring/summer 2017. Based on the interview results, mockups for potential Archistar configuration UIs were developed and evaluated with cognitive walkthroughs in two iteration cycles for answering *RQ2* and *RQ3* in summer 2018. The evaluations also allowed for further elicitation and refinement of user requirements (addressing *RQ1*).

Participants in all end user studies were system admins and technically skilled users, whose participation was entirely voluntary with the motivation to contribute to science and no compensation was paid.

As no sensitive personal data were collected in the studies, no ethical approval was needed according to the Swedish Ethics Review Act.

3.1 Interviews

3.1.1 Interview objectives. For the purpose of end user requirement elicitation, we decided on the following areas of inquiry for our structured interviews:

Security protection goals for the users' applications: Data within organizations typically vary in terms of required type and level of protection. Thus, information classification may be used not only for compliance or legal reasons but also to determine which type of protection is appropriate for each type of data. As suggested by Krutz and Vines (2010), we used a high-medium-low classification scheme based on information security requirements in terms of confidentiality, integrity and availability to determine the protection goals for the interviewees' data.

How/where to distribute data chunks geographically: We investigated how the respondents stated their requirements for the geographical distribution of chunks in relation to their protection goals.

Applicability of secret sharing: The level of security/privacy and cost may vary depending on the cloud deployment model (e.g. private, public or community cloud) (Goyal, 2014), meaning that different security measures may apply to different cloud solutions. Therefore, we wanted to investigate the experts' views on the applicability of secret sharing for different deployment models.

Security measures and trade-offs: We were interested to analyze to what extent users would rely on secret sharing as an alternative to encryption, and whether there were any preferences/priorities in regard to the protection goals of security, privacy and costs (which may be in conflict with each other). Insights into the end user's preferences may help to find configurations that provide a suitable trade-off between conflicting goals.

Factors of trust in CSPs: Based on the non-collusion assumption, the trustworthiness of individual CSPs is less crucial than in a single cloud solution. However, a solution providing great security/privacy does not necessarily result in high *user trust* (Nissenbaum, 1999). Lack of trust may prevent service adoption. Hence, the user needs to trust the Archistar solution for it to come to great use. Privacy can be assured, for example, via the use of "Privacy Seals" – that is, a stamp of approval from a third party that verifies the service provider's privacy compliance and protection guarantees (Pearson and Elahi, 2011). Another indicator of trust may be reputation or trust ratings. When a user lacks a history of direct interaction with an application/organization, they may assess its trustworthiness via

experiences of others (Nissenbaum, 1999). In the interviews, we wanted to analyze the impact of such privacy compliance and trust indicators on the interviewee's trust in CSPs.

3.1.2 Demographics and background. A total of 16 individuals were interviewed, either in person or through video conferencing. Of the 16, 12 respondents were based in Sweden, 2 in Germany, 1 in Austria and 1 in Italy. The respondents were recruited through snowball sampling. They had previous experience with cloud storage and represented system administrators – or IT-experts qualified to conduct system administration work. Interview questions were supposed to be answered from an organizational point of view. If the respondents were only able to answer from a private use-perspective, then we considered their responses still as valuable input for the study.

Among the respondents were a German *Software Developer* and a *Security Engineer* at a multinational IT-company. Two respondents had a profession involving customer support in Sweden; one as an *IT Consultant*; and one as a *Manager in Consulting* that provided security services/products to customers. Two respondents had previous knowledge of Archistar, as their organizations intended to use the solution in the future; one of them was a *Capacity Manager* at a regional ICT provider in Italy and the other a co-founder of a start-up cloud infrastructure company in Austria. Moreover, we interviewed five *PhD students*, two *Lecturers* and one *Professor from a Swedish University* – all within the area of Computer Science. Other respondents were one *IT-Security Coordinator* and one *Project Leader/IT architect*, both of which were knowledgeable in how data backups are stored and handled at their respective universities in Sweden. None of the respondents was involved in the PRISMACLOUD project.

3.1.3 Interview setup. Before starting the interview, each respondent was shown an introduction video[2] to be familiarized with secret sharing. They were informed about the purposes and circumstances of the study and provided informed consent for data collecting and voice recording during the interviews.

The interview included both open- and closed-ended questions. They were asked orally while simultaneously presented in a fillable PDF form, so that the respondents could answer both in spoken and written form.

The questions were sometimes slightly changed or presented in a different order. Follow-up questions (outside of the PDF form) were sometimes asked when clarifications were needed. The interview had been estimated to take 40 minutes. To keep within this time frame, each section in the questionnaire was given a specific number of minutes in which they should be answered. All sections were covered during each interview, but every question in the PDF form was not always asked because of the time limit.

3.1.4 Results from the interviews. This section describes the main results from the interviews, especially in regard to preferences brought up by several respondents.

3.1.4.1 Storage habits and protection goals.

- *Most respondents stored more than one data type in the cloud*: In all, 15 respondents indicated that cloud storage was used for more than one type of data or purpose. Common answers were: documents, code/projects, photos, publications and general data backups.
- *Data with high requirements for availability and confidentiality/integrity may be stored in the cloud*: In all, 15 respondents stored a type of data in the cloud whose *availability* could be valued to the same extent as its *confidentiality* and/or *integrity*. Nine stated that the highest level of requirements was needed for availability and at least one of the other parameters.

- *Most respondents prioritized protection against one data threat over another*: In all, 11 respondents selected "Data Loss" as more severe than "Breaches of Data Confidentiality" – or *vice versa*. Four respondents had previous experience of losing data, either in traditional or cloud-based storage. However, when it came to data breaches, four respondents stated that they were unaware of whether or not they had been subject to such a threat.
- *Cost may be critical*: Five respondents indicated that the proposed solution has to be cost-beneficial for them to use it. In contrast, five other respondents seemed to think that cost was less crucial, either because they were not in a position where they would have to pay for the solution within their organization or because they saw a trade-off with security. One of them still acknowledged that cost could be important for others.

3.1.4.2 Geographical distribution.

- *Implications of different values on k may be unclear*: Eight respondents described aspects that would influence their requirements in terms of total number of chunks (N) and threshold for data reconstruction (k). Several respondents mentioned the *trustworthiness of CSPs*, *availability of individual clouds* and *data sensitivity*. Five respondents considered what different values on N could implicate; four of them suggested that a higher number of chunks could result in *higher costs*. Furthermore, *lower risk of data loss* and *higher processing time* was mentioned by one respondent each. However, only two respondents appeared to reflect upon the consequences of different values on k and in general the impact of k seemed to be less clear. Therefore, values selected by the majority seemed to be arbitrary rather than definite. During the interviews, respondents was informed that the minimum values were $N = 3$ and $k = 2$. Five respondents kept these values for all data types. Six other respondents suggested several combinations of N and k, all of which included the minimum values as a potential option. The highest selected values were $N = 12$ and $k = 5$ and were suggested by a respondent who had previous familiarity with secret sharing.
- *Divided answers on question about minimum distance*: When asked about the minimum distance between data centers, the respondents had the options to specify a distance in *kilometers* and/or *administrative level*. Of all, 14 respondents specified an administrative level, whereas only 8 answered in kilometers. Of received answered, "Different Countries" and "100km" were the most frequent and were suggested by nine and four respondents, respectively. The respondents that selected the same minimum distance in kilometers did not necessarily specify the same requirements in terms of administrative level.
- *Europe, Canada and Australia and New Zealand, most trusted areas for preventing both data loss and breaches*: The top trusted countries/regions for preventing data loss were: (1) Rest of Europe (that is, areas outside South/southeastern Europe), (2) Canada, (3) Australia and New Zealand, (4) the USA and (5) Japan. Mentioned reasons involved the infrastructure's reliability, laws/regulations, political stability and/or simply the safety from natural disasters.

The top trusted countries/regions for preventing breaches of data confidentiality were: (1) EU (including EEA), (2) Canada, (3) Australia and New Zealand, (4) Japan and (5) the USA. Laws/regulations and political stability (including factor such as democracy and corruption level) were once again the most common reasons.

3.1.4.2 Trust in cloud storage providers.

- *Contradictions regarding the trustworthiness of CSPs*: Nine respondents stated that they, as a secret sharing user, would consider utilizing CSPs that they normally would not trust in a single cloud solution. However, all nine argued that it was important that CSPs follow privacy legislations. Moreover, five of them thought it was important that the CSPs have a trust/privacy seal, and seven of them thought it was important that CSPs have high trust ratings.
- *Mixed level of concerns regarding collusion*: Seven respondents expressed that they were concerned that CSPs will collaborate and reconstruct data behind their back, while six respondents stated the opposite.
- *Distribution to EU/EEA countries may be required to prevent collusion and to increase trust*: When asked to select three countries to prevent collusion between CSPs, five respondents chose nations that were all located in EU/EEA, while three respondents selected two EU/EEA-countries and four respondents selected one. The reasoning for the selection involved regulations/laws, political relationships, countries' trustworthiness and publically known incidents in the past. When the respondents were asked about which privacy laws the CSPs should follow, ten respondents answered "EU legislations". Eight respondents also suggested that CSPs should be compliant with local/national laws of a specific country (e.g. Germany).

3.1.4.3 Applicability of secret sharing.

- *Secret sharing may be adequate and beneficial for private clouds*: Six respondents stated that secret sharing, as a security measure, would be adequate for private clouds and fivr respondents indicated that they would benefit from or be interested in using it. One respondent only saw benefits for private use, while two respondents thought it was unnecessary all together. Three respondents seemed skeptical about the claim that, for example, only the data owner would be able to reconstruct the data.
- *Secret sharing may be inadequate for public clouds*: When asked whether secret sharing is secure enough for public clouds, three respondents stated that it was and six respondents indicated that it would not be (perceived as) sufficient.
- *Secret sharing potentially not trusted by public bodies in community clouds*: Three respondents thought secret sharing would be adequate for community clouds with public bodies, but one of them pointed out that these institutions have too high security standards to actually *trust* it. Three respondents argued that it would not be secure enough. One argued that province governments and city councils do not have a high IT maturity, while another one stated that they are too conservative and would not trust such a solution.

3.1.4.4 Preferred security measures.

- *Secret sharing inadequate for sensitive data*: Only two respondents stated that they would like to use only secret sharing to protect *all* their data in the cloud. However, both pointed out that if they were to store sensitive data in the cloud, then they would like to combine secret sharing with encryption. Similarly, four other respondents described that encryption would be needed for sensitive/classified information. Mentioned example were data in health-care applications and documents that only an employer should be able to unlock.

- *Encryption perceived as stronger protection than secret sharing*: Five respondents argued that data would be better protected with encryption than secret sharing. One of them worked for a company that provided data storage to its clients and a customer–managed encryption key could therefore be required by legislations. Another one argued that authorities and institutions should always use encryption, as this is the only adequate protection against data breaches. Three respondents stated that they would like to use only encryption for cloud data.
- *Secret sharing combined with encryption seen as the best protection*: Although some seemed satisfied with just encryption, 12 respondents recognized that a combining secret sharing with encryption, and by this adding protection against unauthorized data reconstruction because of collusion, would be the best solution. Six of them preferred to use both security measures for all cloud data. Two admitted that both security measures would be needed simply because they did not have sufficient knowledge about how secret sharing would work in reality.

Numerous respondents indicated that they needed to know more about Archistar to give definite answers on the interview questions. Their trust in the solution may depend on:

- the organization behind it;
- if one can prove that data are protected according to its classification and that one cannot extract any information by gathering one chunk;
- if one can share information with others without giving out the login to one's user account;
- if one can assure that data are not lost/inaccessible when it is needed; and
- where data are reconstructed; if chunks are combined in the secret sharing application, then there would still be a single target point for attackers.

3.1.4.5 Requirements. Some of the main requirements for the configuration UIs that we could elicit from the interviews can be summarized as follows:

- Different configurations should be enabled addressing varying end user preferences in terms of protection goals, costs, trust in CSPs and geographic distributions of CSPs based on political or legal domains, climate zones and/or geographic distances.
- Any privacy and/or trust seals or ratings should be easily recognizable when the user has the choice to select CSPs.
- Guidance for selecting the parameters N and k, for example, by providing suitable pre-settings, is needed.
- Secret sharing should be combined with encryption as a default for data with high confidentiality or privacy requirements.
- Hybrid clouds may support organizations that for privacy reasons do not want to rely on public clouds with at least one chunk to be retrieved from organization's own storage.

3.2 Design and evaluation of configuration user interfaces

3.2.1 First version of mockups

3.2.1.1 Mockups. A first version of configuration UI mockups were designed addressing the elicited requirements, particularly in terms of providing suitable pre-settings for varying

end user preferences. The mockups consisted of three steps: As the interviews showed that most respondents could prioritize one protection goal over another, in the first step of the UI, the users were asked to prioritize the protection goals "Cost Minimization – Low costs," "Data Protection – High Confidentiality" and "Data Loss Protection – High Availability" from most to least important (Figure 1). Based on this prioritization, default values for the number of chunks N and the threshold k were provided by the UI with a suggestion how the number N of chunks should be distributed to the public and private cloud. In a second step, the user had the option to add encryption for confidential data. In Step 3, the configuration could be fine-tuned in dependence on the available budget and estimated storage size. The secret sharing could be changed from CSS to Shamir's scheme. Geographic restrictions could be fine-tuned with the help of a map with added layers to graphically represent trade blocs, internet infrastructure as well as risks for natural disaster. Moreover, information about service offering and creditability of selectable storage nodes and any legal restrictions was provided for the map.

3.2.1.2 Evaluation. The first version of UI mock-ups was evaluated with five individual walkthroughs. The participants constituted one *Administrative Director* at a municipality's IT department, one *IT Security Coordinator* at a Swedish University, who also had the position of a *Data Protection Officer* (DPO), two *System Administrators* at a Swedish University, and one *IT Security Expert*, who worked part-time as a security consultant in industry for many years. They were selected and invited via personal contacts because of their complementing expertise.

Before each session, each participant was first briefed about the purpose of the study, asked to provide informed consent for the participation, data collection and for voice recording during the interview sessions. The participants were then given a short verbal introduction to Archistar and were shown the introduction video used in the previously conducted interviews.

During the walkthroughs, the participants were assigned to create a configuration for a typical data backup/archiving project in their organization. On each step in the

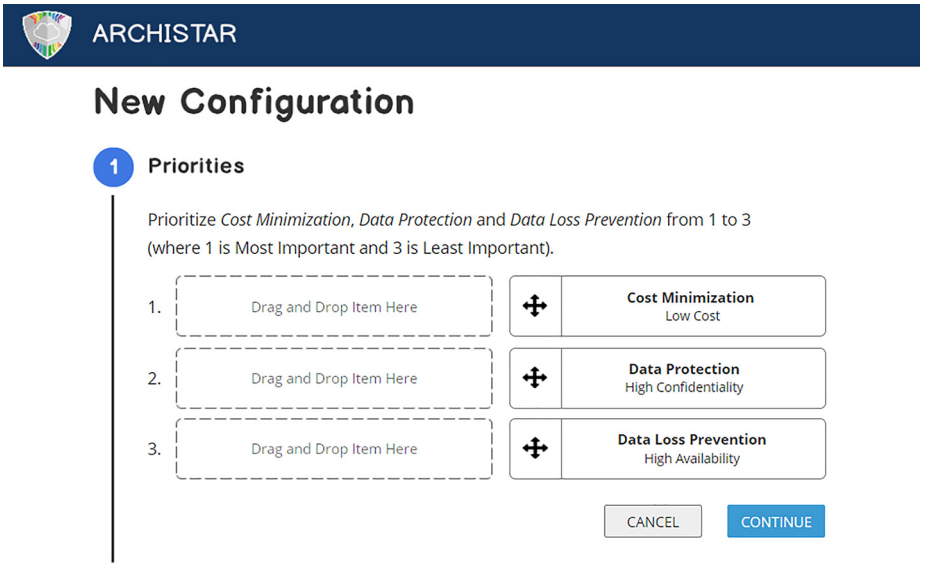

Figure 1.
Mockups Version 1 – prioritizing protection goals

configuration process, the respondents were asked about the perceived meaning and relevance of UI elements as well as the feasibility of the proposed solution.

3.2.1.3 Main evaluation results.

- Three participants perceived "High Data Confidentiality," "High Data Availability" and "Cost Minimization" as a sufficient set of protection goals for the Archistar configuration. However, the ambiguity of "High Data Availability" was pointed out, which could refer to either or both 24/7 uptime and quick access time. However, one participant proposed to rather select the protection goals in relation to the user's needs, particularly in terms of how confidential the data actually are and the actual budget, rather than making any prioritization. Also, a request for prioritization may not clearly mediate that Archistar provides high confidentiality and availability protection by default.
- Four participants thought it was sensible to allow administrators to select the geographical destination of each data chunk. However, multiple participants argued that the selection should be made from a *list* rather than a *map*, which may appear less accurate, for example, in terms of showing the risk of floods or fires.
- Two participants explained that they would only be able to choose CSPs with which their organization has a procurement contract and/or (in case of personal data) a data processing agreement. However, establishing such contracts is rarely the administrators' responsibility but rather a management decision.
- Three participants thought that the budget should be determined *before* the configuration, while two other explained that they as system administrators were not responsible for budgeting decisions at their organization, which is also rather up to the management.

3.2.2 Second version of mockups

3.2.2.1 Mockups. The second mockup version addressed comments from the first evaluation round. In particular, the UI was split to adhere to two types of roles: The first part of the UI would be utilized by individuals with a "manager" role to establish global settings for all archiving projects within an organization, in particular related to existing contracts and budget restrictions. These global settings would serve as a filter, preventing system administrators from utilizing non-contracted CSPs or exceeding the organization's budget.

A second part of the configuration UI would be used by users in the "system administrator" role to make configurations meeting the protection preferences for specific storage projects. In this part, the administrator would simply select key protection goals to indicate whether additional protection packages should be added in addition to Archistar's base protection, without putting these key protection goals in a specific priority order. The key protection goals were "Enhanced Confidentiality," "Enhanced Access Time" and "Enhanced Data Loss Prevention." Each of them was represented in the UI with a checkbox and a tool tip with information about the type of data for that the additional protection package would be suitable for. Further advanced configuration setting could then be done by clicking "Enter Expert View" (Figure 2).

3.2.2.2 Evaluation. The second version of the mockups was evaluated through follow-up individual walkthroughs with three participants – that is, one IT Security Coordinator at a Swedish University, who also had the position of a DPO, one system administrator at a Swedish University, as well as one security expert, who worked part-time as a security consultant in industry. All of them participated in the walkthroughs of the previous version of the mockups. They were asked to contribute to an inspection of the second mockup

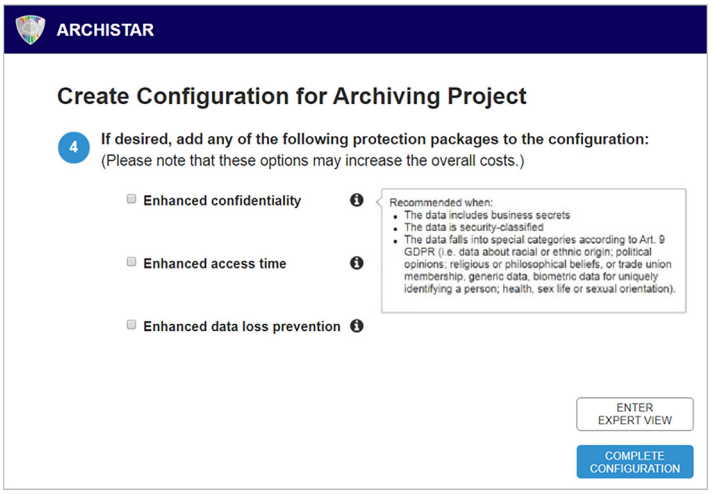

Figure 2.
Mockups version 2 – adding protection packages

version for two reasons: First, all contributed with their different experiences, that is, the DPO contributed with experiences from the organizational management side and the other two participants as security experts from the university (government) and from the industry perspective. Second, the three invited participants were also those who had made essential comments, which we tried to address with the second version. We were, therefore, in particular interested to receive feedback on whether we addressed their comments from the first evaluation round adequately.

3.2.2.3 Main evaluation results.

- All participants confirmed it was appropriate to split the UI into to two parts, that is, one for Managers and one for Administrators. Participants also confirmed that it was appropriate to request separately in the Manager's UI to specify procurement contracts and data processing agreements, which the organization has established with CSPs either directly or via cloud brokers/mediators. It was stated that data processing agreements are typically included in the procurement contracts, but data processing agreements may also exist on their own, especially if the customer is a private company.
- Two participants argued that the extent to which confidentiality, availability and cost would be impacted by the protection packages (that could be added to the base protection) was unclear in the Administrator's UI. It was also stated that the option to add protection packages may give the impression that the base protection is inadequate. A comparative view (before and after the package is added) with feedback on costs could help users to understand the implications.
- Rather than selecting additional protection packages, two participants argued that the UI should allow the user to specify directly what type of data will be archived and the need for additional protection packages should subsequently be determined by the *system* itself. They, thus, argued for a "data type driven" configuration approach. Such an approach should provide extra guidance and prevent that users could otherwise too easily opt for additional protection packages, which might

result in extra costly security measures taken that would be higher than needed for the data to be protected.

4. Human computer interaction guidelines and discussion

The main results of our user studies lead to the following Human Computer Interaction guidelines that we recommend for configuration management user interface for Archistar (or any other Multi-Cloud Storage Applications based on Secret Sharing):

4.1 Two configuration user interfaces are needed

Many choices to be made depend on procurement contracts, existing data processing agreements or financial restrictions for the organizations that system administrators or project leaders are not aware of or do not have the authority to decide upon. Hence, the configuration UI should be divided into two parts enabling:

- global configuration settings in regard to contracts (procurement contracts, data processing agreements pursuant to the GDPR) and/or costs in terms of the overall available organizational budget for data storage projects to be made by managers within the organization; and
- specific configuration settings for each storage project by the system administrators; the latter typically comprises all security-related settings but could optionally also allow to specify project-related budget restrictions.

The global configuration settings by the management should be done directly after Archistar's installation and set a filter for the selectable CSPs.

The remaining HCI guidelines relate to the project-related settings to be done by system administrators.

4.2 Make clear that protection is high by default

The start page UIs for the storage project-specific configurations has to clearly signal to the users that Archistar is by default providing a high protection of security and privacy for the outsourced data. Any additional protection packages offered under the project-specific configuration UI may cause users to have less confidence in the system's base protection. More protection packages than needed may, therefore, be selected, resulting in extra costs. Therefore, the start page should help to clarify that choosing additional protection options later when configuring the system will only increase this base default protection for the cases where data that need special protection and that even without extra protection measures, the data will be well protected. Figure 3 provides an example of a start page. Trust in Archistar and its default base protection may be enhanced if a privacy/security seal is obtained for Archistar and prominently displayed, as shown in Figure 3.

4.3 Automatically set parameters and solve trade-offs

Storage project-specific configuration parameters including server locations that are providing suitable trade-offs for all protection goals that need to be made should be determined automatically based on the requirements that the user specifies via the configuration UI. Selecting suitable parameters N (total number of chunks) and k (threshold of data reconstruction) requires in-depth knowledge about secret sharing and even technically skilled users should not be assumed to have such expert knowledge. Moreover, other settings for choosing CSPs even require for instance legal privacy expertise in regard

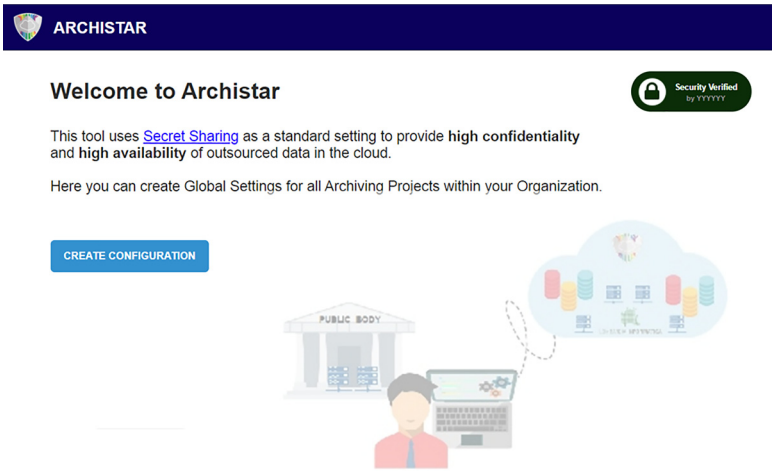

Figure 3.
Start page for the storage project-specific configurations

to server locations and the needed level of protection pursuant to the GDPR. Therefore, these configuration parameters and settings should be selected based on stated user requirements, while at the same time, users should still have the option to view and adjust the configurations later.

4.4 From protection goal-based to project and data type-based settings

For automatically setting the configuration parameters, we suggest to use a data type-driven approach. The UIs that we have thus developed have evolved from (1) a configuration UI that asked directly for the user's protection goals/preferences to determine appropriate values for configuration parameters (Figure 1) to (2) a UI that provided guidance via tooltips by indicating which types of data the selectable protection goals were suitable for (Figure 2) and, finally, to (3) our recommended UI that instead asks the user for the type of data that will be stored in the cloud (Figure 4). The reason for this was that users did not only have difficulties to set parameters like k and N or to determine suitable server locations meeting their requirements, but they perceived it as difficult to specify more high-level protection goals for their data. Therefore, based on the information about the data types that the user has to specify in the UI, the configuration system should also help them to determine first the required protection levels and second, based on this, suitable trade-offs and related configuration settings.

As shown in Figure 4, instead of asking the user about data protection requirements in terms of enhanced protection of data confidentiality or availability, the need for enhanced protection is rather determined based on the type of data to be stored in the cloud. If for instance special categories of data (i.e. sensitive personal data) pursuant to Article 9 of the GDPR, then business secrets or security classified data are to be stored in the cloud (DataType 1); enhanced confidentiality measures have to be added for guaranteeing appropriate protection. In this case, it would be automatically determined for the Archistar configuration settings that data encryption is used in addition to secret sharing, that a higher threshold k is used, that the servers will be located in the EEA (or in another country for that an adequacy decision exists pursuant to Article 45 GDPR unless exceptions of Article 46-49 GDPR apply that would legitimize the data transfer) and that at least one

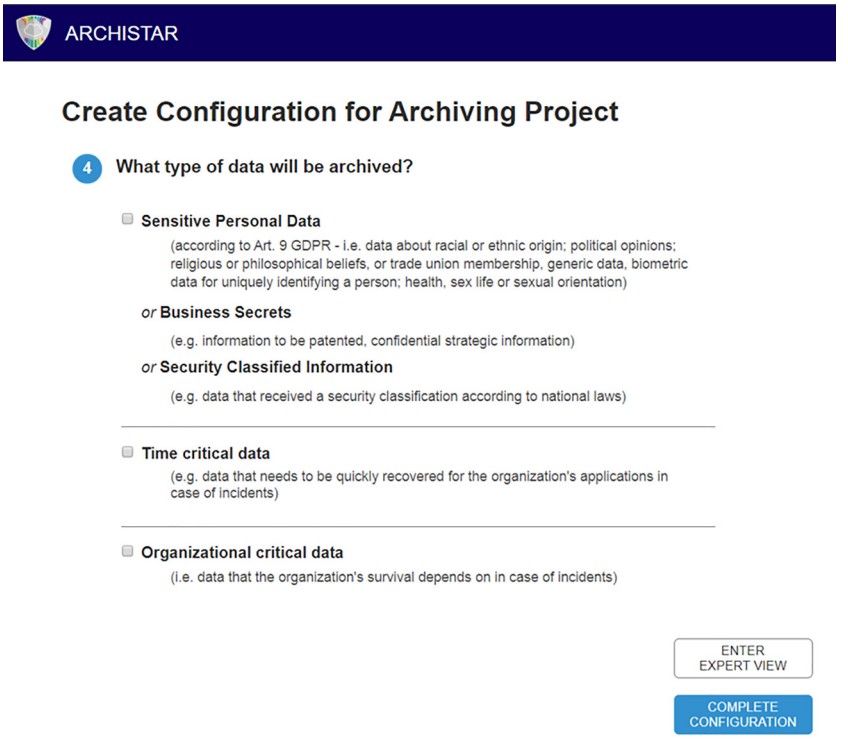

Figure 4.
Data-driven approach for determining configuration settings

chunk needed to reconstruct the data is placed in the private cloud of the user's organization. For time-critical data that need to be quickly recovered in case of an incident (DataType 2), the number N of servers and distances to the servers chosen should be kept low, and servers with high up-time guarantees should be selected. Finally, for organizationally critical data (DataType 3), which are essential for the survival of an organization in the case of an incident, the redundancy (*N-k*) should be increased and servers with high ratings in terms of contingency plans and disaster recovery guarantees should be chosen. In Table I., we provide a suggestion of how the secret sharing parameters k and N, suitable trade-offs for those parameters and other security-related settings can be assigned for combinations of the three different selectable data type options in Figure 4. These configuration settings are determined based on the protection needs for the data type: DataType 1 requires enhanced confidentiality, DataType 2 enhanced disaster recovery preparedness and DataType 3 enhanced data loss prevention. If procurement contracts exist in public organizations, then the list of selectable servers is further restricted accordingly.

A data-specific approach is recommended not only for choosing additional protection packages but also for determining the needed storage space, as also suggested by our test participants.

4.5 Include an expert view for changing technical settings

While the configuration system automatically determines suitable configuration setting, expert users should still have the possibility to view those settings and adjust them via an

Data type options and combinations	Secret sharing parameters k/N and other protection settings
(*DataType 1*: Sensitive personal data, business secrets, security-classified data; *DataType 2*: time-critical data; *DataType 3*: Organizational critical data)	(k: threshold, N: no of servers)
DataType 1	4/5, two servers from private cloud and three from externals CSPs with data processing agreements, all servers located in the EEA; additional use of encryption
DataType 1 and DataType 2	4/5, two servers from private cloud and three from externals CSPs with data processing agreements, all servers located in the EEA and preferably (i.e. if available) with a low distance from the user's location and high uptime guarantees; additional use of encryption
DataType 1 and DataType 3	5/7, three servers from private cloud and four from externals CSPs, all servers to be placed in the EEA but in different geographic areas and preferably with good incident management ratings; additional use of encryption
DataType 1 and DataType 2 and DataType 3	4/6, three servers from private cloud and three from externals CSPs, all servers to be placed in the EEA but in different geographic areas, however still in a low distance from the user's location and preferably with good incident management ratings and high up-time guarantees; additional use of encryption
DataType 2	2/4, servers have a low distance from the user's location and high up-time guarantees; fast caching can be realized by storing two chunks on local servers (If personal data: only CSPs with data processing agreements, all servers located in the EEA)
DataType 2 and DataType 3	2/3, servers from different geographic areas, preferably with good incident management ratings and high uptime guarantees (If personal data: only CSPs with data processing agreements, all servers located in the EEA)
DataType 3	3/5, servers to be placed in different geographic areas with good incident management ratings (If personal data: only CSPs with data processing agreements, all servers located in the EEA.)
No data type option selected	2/4 (If personal data: 3/5, only CSPs with data processing agreements, all servers located in the EEA.)

Table I. Choice of security parameters for different combinations of data types that can be selected in Figure 4

expert view that can be opened upon demand, for example, they could also choose encryption for data that are not of DataType 1. Adjustments may, however, only be permitted as long as they do not restrict the protection needed for the chosen data types.

In this expert view, we suggest to show a map view only on demand and to show instead per default a table view of the selectable CSPs. This table should include information about server locations, any ratings or certifications about disaster preparedness, any incident reports, any trust or privacy seals and access time/uptime guarantees.

4.6 Direct feedback on costs

The expert view should also provide feedback on costs that result from the determined or chosen configuration settings.

5. Related work

Related work on decision support systems in multi-cloud application and cloud federation which address or consider security aspects include in particular the following approaches: A decision support method for multi-cloud applications has been developed in Omerovic *et al.* (2013), which considers risk, quality and cost factors to assist decision-makers in choosing provider and services. A first systematic step towards decision support for cloud migration was presented in Andrikopoulos *et al.* (2013). They identified four major decision points and tasks which need to be performed to support the decision. CloudDSF (Andrikopoulos *et al.*, 2014) is a refinement including a visualization of this approach. The Cloudstep process for cloud migration (Beserra *et al.*, 2012) uses an approach based on process profiles and apply the concept of cloud adoption patterns. They try to manage the technical and non-technical risks for cloud migration of legacy applications. An automated approach for decision support in cloud migration has been presented in Amato and Venticinque (2013). This system can select the best matches from offers received in machine readable form against a multi-objective function. However, all these approaches are not addressing our concrete problem. In the case of multi-cloud storage, the decision support must be able to combine the different offerings into a new virtual service with a new SLA stronger than the individual ones it is composed of. Additionally, it should also interactively involve the user in the decision process and communicate the features to the system manager. A dedicated approach for dispersed storage systems has been presented in Mansouri *et al.* (2013) focusing on finding a cost optimal solutions for given quality of service to reduce overall pricing. However, this approach does not target security as an objective but has the objective to maximize the profit for providers.

Other related work on using secret sharing for secure cloud storage, as for example, surveyed in Attasena *et al.* (2017), has not addressed the usable configuration management problem yet.

To the best of our knowledge, no work on the end user aspects and usable design of a DSS in multi-cloud applications based on secret sharing exists. We try to fill the gap by the human-centered design of an active or even cooperative DSS which is easy to use and supports users in cloud adoption for storage applications.

6. Conclusions

This paper presents the results of our user studies for providing guidelines for a usable design of configuration management UIs for the Archistar framework. The guidelines show how users can be assisted with an easy to use configuration meeting their privacy, security, trust and other organizational requirements.

Overall, we could conclude that Archistar configurations do not primarily require detailed technical knowledge or organizational knowledge and legal expertise. Especially, the management within organizations needs therefore to be involved in providing input for global configuration settings. We conclude that moving to an automatic data-based configuration (instead of a protection-goal based one) will lead to UIs that also make the configuration easy to use for non-technically skilled project leaders or even lay users, as no technical settings and choices will be required any longer for the configuration UI shown by default. Hence, even though we initially assumed that we need to have different types of configuration UIs for lay users and for technically skilled users, our user studies showed that as the Archistar configuration is a complex task, even technically skilled users need special guidance, which can be provided through our data type-centric approach.

Notes

1. https://prismacloud.eu/
2. www.youtube.com/watch?v=4_jx2V1z-2U

References

AlZain, M.A., Pardede, E., Soh, B. and Thom, J.A. (2012), "Cloud computing security: from single to multi-clouds", *Proceedings of the Annual HI International Conference on System Sciences*, *IEEE*, pp. 5490-5499.

Amato, A. and Venticinque, S. (2013), "Multi-objective decision support for brokering of cloud SLA", *Proceedings – 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013*, *IEEE*, pp. 1241-1246.

Andrikopoulos, V., Strauch, S. and Leymann, F. (2013), "Decision support for application migration to the cloud – challenges and vision", *Proceedings of the 3rd International Conference on Cloud Computing and Services Science – Volume 1: CLOSER*, *SciTePress*, pp. 149-155.

Andrikopoulos, V. Darsow, A. Karastoyanova, D. and Leymann, F. (2014), "CloudDSF – the cloud decision support framework for application migration", Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8745 LNCS, pp. 1-16.

Attasena, V., Darmont, J. and Harbi, N. (2017), "Secret sharing for cloud data security: a survey", *The VLDB Journal*, Vol. 26 No. 5, pp. 657-681.

Beserra, P.V., Camara, A., Ximenes, R., Albuquerque, A.B. and Mendonça, N.C. (2012), "Cloudstep: a step-by-step decision process to support legacy application migration to the cloud", *2012 IEEE 6th International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems, MESOCA 2012*, *IEEE*, pp. 7-16.

Bessani, A. Correia, M. Quaresma, B. Andre, F. and Sousa, P. (2011), "DepSky: dependable and secure storage in a cloud-of-Clouds", *Proc of Eurosys*, available at: www.navigators.di.fc.ul.pt/archive/papers/eurosys219-bessani_.pdf

Correia, M. (2014), *Clouds-of-Clouds for Dependability and Security: Geo-Replication Meets the Cloud*, Springer, Berlin, Heidelberg, pp. 95-104.

European Commission (2016), European Commission: Regulation (EU) 2016/679 of The European Parliament and of The Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR)." (2016), Official Journal of the European Union, L119, 4 May 2016 first occurrence.

Goyal, S. (2014), "Public vs private vs hybrid vs community-cloud computing: a critical review", *International Journal of Computer Network and Information Security*, Vol. 6 No. 3, p. 20.

Happe, A., Wohner, F. and Lorünser, T. (2017), "The archistar Secret-Sharing backup proxy", *Proceedings of the 12th International Conference on Availability, Reliability and Security, ACM*, p. 88.

Krawczyk, H. (1994), "Secret sharing made short", in Stinson, D.R.(Ed.), *Advances in Cryptology – CRYPTO' 93, 13th Annual International Cryptology Conference, Santa Barbara, CA, August 22-26, 1993, Proceedings*, Vol. 773, pp. 136-146.

Krutz, R.L. and Vines, R.D. (2010), *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing.

Li, M. (2012), "On the confidentiality of information dispersal algorithms and their erasure codes", *ArXiv Preprint ArXiv:1206.4123*, pp. 1-4.

Loruenser, T., Happe, A. and Slamanig, D. (2015), "ARCHISTAR: towards secure and robust cloud based data sharing", *Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference On*, *IEEE*, pp. 371-378.

Lorünser, T., Slamanig, D., Länger, T. and Pöhls, H.C. (2016), "PRISMACLOUD tools: a cryptographic toolbox for increasing security in cloud services", *Availability, Reliability and Security (ARES), 2016 11th International Conference On*, *IEEE*, pp. 733-741.

Mansouri, Y., Toosi, A.N. and Buyya, R. (2013), "Brokering algorithms for optimizing the availability and cost of cloud storage services", *Proceedings of the International Conference on Cloud Computing Technology and Science*, *CloudCom*, *IEEE*, Vol. 1, pp. 581-589.

Nissenbaum, H. (1999), "Can trust be secured online? A theoretical perspective".

Omerovic, A., Muntés-Mulero, V., Matthews, P. and Gunka, A. (2013), "Towards a method for decision support in multi-cloud environments", *4th International Conference on Cloud Computing, Grids, and Virtualization (CLOUD COMPUTING 2013)*, pp. 162-180.

Pearson, S. (2013), "Privacy, security and trust in cloud computing", *Privacy and Security for Cloud Computing*, Springer, pp. 3-42.

Pearson, S. and Elahi, T. (2011), "Privacy assurance checking", *Digital Privacy*, Springer, pp. 427-456.

Ren, K., Wang, C. and Wang, Q. (2012), "Security challenges for the public cloud", *IEEE Internet Computing*, Vol. 16 No. 1, pp. 69-73.

Shamir, A. (1979), "How to share a secret", *Communications of the Acm*, Vol. 22 No. 11, pp. 612-613.

Stangl, J., Lorunser, T. and Pudukotai Dinakarrao, S.M. (2018), "A fast and resource efficient FPGA implementation of secret sharing for storage applications", *2018 Design, Automation and Test in Europe Conference and Exhibition (DATE)*, *IEEE*, pp. 654-659.

Yu, S. Wang, C. Ren, K. and Lou, W. (2010), "Achieving secure, scalable, and fine-grained data access control in cloud computing", *INFOCOM 2010*, pp. 534-542.

About the authors

Erik Framner has been a Researcher at the Computer Science Department of Karlstad University, which he joined in 2016 after graduating in Information Systems at Karlstad University. He is specialized in Interaction Design and usable privacy research and has been contributing to the HCI research and development activities in the EU H2020 projects PRISMACLOUD and CREDENTIAL.

Simone Fischer-Hübner has been a Full Professor at Karlstad University since June 2000, where she is the head of the Privacy & Security (PriSec) research group. She received a Diploma Degree in Computer Science with a minor in Law and a PhD and Habilitation Degree in Computer Science from Hamburg University. She has been conducting research in privacy and privacy-enhancing technologies for more than 30 years. She is the Chair of IFIP WG 11.6 on "Identity Management", the Swedish IFIP TC 11 representative, member of MSB's Information Security Advisory Board (MSB:s informationssäkerhetsråd) and Vice Chair of IEEE Sweden, Computer/Software Engineering Chapter. She is partner in several European privacy-related research projects including the EU H2020 projects PAPAYA, CREDENTIAL PRISMACLOUD and the EU H2020 Marie Curie ITN Privacy&Us, for which she is also the scientific coordinator. Moreover, she coordinates the Swedish IT Security Network SWITS. Simone Fischer-Hübner is the corresponding author and can be contacted at: simone.fischer-huebner@kau.se

Thomas Lorünser (Dipl.-Ing.) is Scientist and Project Manager of the Center for Digital Safety and Security at AIT (Austrian Institute of Technology). He has a research background in information and cyber security as well as applied cryptography. During the past 15 years, he successfully managed various national and international research projects from medium to large scale in network and cloud security. He has coordinated the EU funded H2020 research project PRISMACLOUD.eu comprising 16 international partners. He also teaches selected topics in Cloud Computing, Internet of Things and IT Security as lecturer at two universities of applied sciences and actively contributes to security standards in the International Organization for Standardization (ISO, JTC1/SC27).

Ala Sarah Alaqra has since 2015 been a PhD Student and Researcher at the Privacy & Security (PriSec) research group of Karlstad University, where she has contributed to the HCI research of the PRISMACLOUD EU H2020 projects. She holds a Master Degree in Computer Science from Umeå University and a Licentiate Degree from Karlstad University. Her research focusses Human Computer Interaction and usable privacy.

John Sören Pettersson is a Full Professor at Karlstad University in Sweden where he heads the Information Systems research group. He has for the past two decades researched means and concepts of interactivity in prototyping. The primary application areas of his research are within the fields of usable privacy, mobile communication for development and IT support for management training in crisis response. He has contributed to the usable privacy research of several EU projects, including PRISMACLOUD and CREDENTIAL.