Proceedings of the Tenth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2016)

Stakeholders' Perspectives on Malleable Signatures in a Cloud-based eHealth Scenario

A. Alaqra, S. Fischer- Hübner, J.S. Pettersson and E. Wästlund

Karlstad University, Karlstad, Sweden
e-mail: alaa.alaqra@kau.se

Abstract

In this paper, we discuss end user requirements that we elicited for the use of malleable signatures in a Cloud-based eHealth scenario. The concept of a malleable signature, which is a privacy enhancing cryptographic scheme that enables the redaction of personal information from signed documents while preserving the validity of the signature, might be counter-intuitive to end users as its functionality does not correspond to the one of a traditional signature scheme. A qualitative study via a series of semi-structured interviews and focus groups has been conducted to understand stakeholders' opinions and concerns in regards to the possible applications of malleable signatures in the eHealth area, where a medical record is first digitally signed by a doctor and later redacted by the patient in the cloud. Results from this study yielded user requirements such as the need for suitable metaphors and guidelines, usable templates, and clear redaction policies.

Keywords

HCI Requirements, Malleable Signatures, Usable Privacy, Cloud tools, eHealth

1. Introduction

In recent years, there has been a continuous trend towards the usage of Cloud storage and Cloud computing, mainly due to increasing needs of users and the advancements of technologies which enables them (Khan et al., 2013; Subashini and Kavitha, 2011). Yet, questions regarding security and privacy continue to emerge, and work on solutions to tackle different aspects of these questions continues to develop (Wei et al., 2014). An important element in this discussion is the user, since the use of proposed solutions and tools is up to the user, and would need to be accepted and comprehended to a certain extent. This imposes a challenge when designing privacy and security enhancing tools, where usability of these tools is at focus. One approach, as seen in this paper, is to address users early on during the design and implementation processes as suggested by (Schaar, 2010) as being important when following a Privacy by Design approach.

The scope of our study is the EU H2020 PRISMACLOUD (Privacy and Security Maintaining Services in the Cloud) project that develops cryptographic schemes to be used for the Cloud, which may be counterintuitive to users, as these solutions either lack real-world analogies or have properties different to the ones of related security solutions.

One example of such a privacy-enhancing crypto schemes is malleable signatures, which allows redaction of personal information from a signed document while preserving the validity of the signature of the document, and which has thus properties different to the ones of traditional signature schemes. Hence, an important goal for the project is to elicit end user requirements using empirical methods in order to address usability aspects and other social factors of services based on such schemes. Our interest was therefore to gain an understanding of end users current expectations and opinions. Hence, the focus was on eliciting requirements from key stakeholders' perspectives, who are representing user groups or are aware of end users' opinions and needs. Consequently, a human centred approach has been adopted and demonstrated by a qualitative study to elicit the requirements for the use of malleable signatures for a Cloud-based eHealth use case within the scope of the research project PRISMACLOUD.

The remainder of this paper is structured as follows: Malleable signatures in the context of an eHealth use case of PRISMACLOUD is described in Section 2. Qualitative methods used in the study are presented in Section 3, followed by results and discussions (Sec.4) of the elicited requirements. Finally, Section 5 sums up with conclusions and discusses future works.

2. Malleable Signatures in eHealth Scenario

PRISMACLOUD is specifically focussing on the research and development of efficient and flexible cryptographic methods that allow the controlled modification and sharing of data in the Cloud. One of these crypto methods are malleable signatures that have a well-defined flexibility property. In collaborative cloud applications, different users often need to modify common data. Traditional electronic signatures are static, meaning that any modification of electronic signed data invalidates the signature. In contrast, malleable signatures allow the controlled modification of the signed text (e.g., by redacting ("blacking out") certain parts of the text) without invalidating the corresponding signature (i.e., preserving the authenticity of the text), see Demirel et al. 2015. In particular, the malleable signature scheme that we study in this paper is characterised by: (1) only controlled modifications are allowed for the data, i.e. for this, the signer can define modification policies in regard to what parts of the text can be modified by whom and with what operations;(2) allowed modifications may be for everyone or may be restricted to persons possessing a specific cryptographic key ("keyed" operations); (3) any modification beyond the defined policies will invalidate the signature and thus the authenticity of the text, although authorised modifications preserve the validity of the signature.

In a typical application scenario of malleable signature schemes, a person ("redactor") is allowed to redact ("black-out") sensitive information from a document without invalidating the original signature, thus maintaining the authenticity of the document. In PRISMACLOUD, this "redaction" application scenario of malleable signature for the eHealth domain is currently developed and was used as a basis for elicitation of requirements in part of our interviews and focus

group discussions. The more detailed steps of this eHealth scenario are as follows (see also Figure 1): In a hospital system, a medical doctor (Doctor A) is upon discharge of the patient from a clinic, defining redactable fields in the patient's medical file, signing it with a malleable signature and then transferring the signed patient file to the patient's account on hospital cloud platform. The patient is allowed to "black-out" sensitive information from her patient file while maintaining the authenticity of the document. For instance, if the patient file contains blood test results in the form of blood values and diagnoses and if the patient wants to get a second opinion on a diagnoses, she could redact the diagnosis fields from the patient file and make the redacted patient file including blood values only available on the cloud platform to a specialist of her choice. The specialist (Doctor B) can then in turn still validate the signature and thus verify the authenticity of the patient's blood value data.

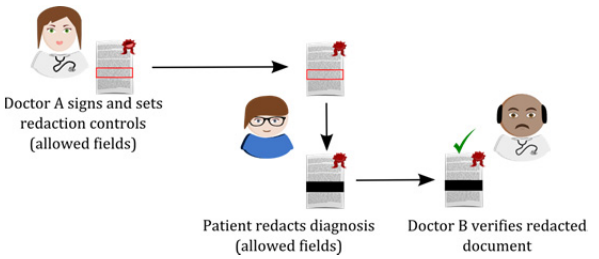

Figure 1: Malleable Signatures in eHealth Scenario

3. User Studies Methodologies

Following a user-centred design (UCD) approach, a qualitative approach was adopted for eliciting requirements using semi-structured interviews and focus group workshops. Additionally, post interview questionnaires were used as quantitative means to provide further insight.

3.1. Semi-structured Interviews

Semi-structured interviews were chosen as a method to capture qualitative data from different key-stakeholders, which are to a large extend representing or understanding the positions of users or user groups, in order to understand their status, needs, opinions, motivations for cryptographic solutions for the Cloud. The flexibility of semi-structured interviews allows exploration and open discussions of key points brought up throughout the interview.

In total, 19 interviews were conducted: 5 for the Smart City, 7 for the eGovernment, and 7 for the eHealth use case. In this paper, we focus on the requirements for the eHealth scenario. In order to capture opinions from different roles within the health sector, the 7 participants were: A general practitioner, security manager, chief executive officer, chief information officer, coordinator, and 2 nurses. The other participants interviewed, for eGovernment and Smart City cases, varied between top

management, technical, and non-technical roles within their organizations; e.g., CEO, IT system management, or lawyer. Interviews were scheduled for 60 minutes including a follow up questionnaire; however the duration of interviews varied between 50 and 190 minutes. There were 1-2 interviewers for each interview. Mainly notes were taken, and some interviewees consented for voice-recording the sessions for later analysis. In discussion workshops at Karlstad University, the authors jointly evaluated the interviews by identifying the main observations and mapping them into end user and usability or technical requirements and, where possible, proposed design solutions for addressing those requirements. The basic structure of the interview consisted of three parts: (1) General inquiry, (2) Case scenarios, and (3) Requirements. In part (1), after briefing the interviewee and getting the consent form signed, inquiries about the interviewees organization and their state of the art in regards to authenticating documents physically and digitally, as well as their experience of Cloud services. In part (2), one of the three target areas scenario (eHealth, eGovernment, Smart City) was chosen corresponding to the interviewee. The case scenario was presented as a context for a discussion aimed at understanding interviewees' expectations, opinions, experiences, and concerns in regards to the cryptographic schemes and functions proposed in the scenario. The final part (3) aimed at eliciting requirements from the interviewees' point of view for a secure, private, trustworthy cloud based system; this was summarised later by the interviewers.

3.2. Focus Groups (workshop)

A workshop with expert focus groups was conducted to gather qualitative data from group tasks and discussions that included malleable signatures and proposed case scenario (eHealth). The aim of the focus group discussions was to explore end user and HCI (Human Computer Interaction) challenges of the case scenarios and further elicit requirements in regards to usability, trust, and privacy. The workshop took place at the IFIP summer school 2015, at Edinburgh University in August 2015. In total 20 expert participants with different research levels and backgrounds, related to privacy and security, from university, government, and industry formed the 4 interdisciplinary focus groups. The workshop consisted of three parts: (a) an introduction to the workshops agenda, materials, group forming, and group members' introductions;(b) discussions about case scenario selections and related cryptographic functions, and further the implications and features of those functions in regards to usability, privacy, and trust; (c) requirements elicitation of cryptographic functions from part (b) to enhance usability, privacy, and trust in the Cloud. Details about the workshop set up, discussion and elicited requirements are presented in Alaqra et al. 2016b.

4. Results and Discussions

This section summarises the main requirements that were elicited via the interviews of eHealth and eGovernment specialists (denoted with the prefixes RH and RG respectively) and via five focus group workshops (denoted with the prefixes R

followed by a number for the respective focus group). A complete elicitation of all requirements can be found in Alaqra et al. 2016a.

In the interviews, it was noted that a distinction between a Hospital platform and Cloud portal has to be made, which is also reflected by the PRISMACLOUD eHealth scenario, and thus the general requirements and observations are sectioned correspondingly. A Hospital platform is defined as the organization internal platform that is confined to only medical staff. The Cloud portal, on the other hand, allows the patients to create accounts and receive shared and authenticated medical documents from the Hospital platform, which they can then in turn share with other stakeholders, such as personal trainers, physiotherapists or their general practitioners on that cloud portal. The interviews mainly contributed to general requirements for the two prospective platforms for addressing end user issues in regards to the security, privacy and trust for signing and handling the patient's personal data. As also the interviews conveyed, different types of general requirements need to be addressed for the different platforms.

For the hospital platform, end user requirements focus on secure authentication of health care professionals and the accountability of their actions as a prerequisite for securely signing and handling of patient data and for enhancing the patient's trust in the hospital side of the eHealth malleable signature application (see section 4.1). End user requirements in regard to the cloud portal focus on the accountability and privacy guarantees of the Cloud provider for enabling patients to establish reliable trust in the Cloud Portal hosting the patient side of the eHealth malleable signature application (section 4.2).

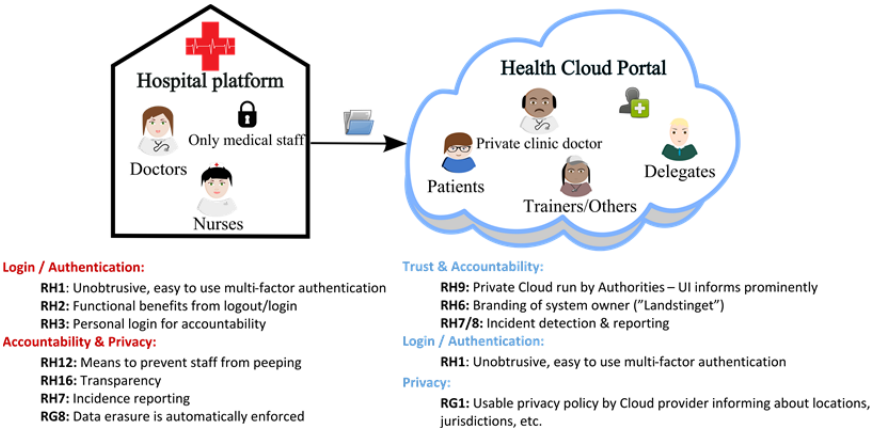

Figure 2: General Requirements for the Hospital Platform (left) and Cloud Portal (right)

Discussions regarding malleable signatures in the interviews were merely informative to the interviewees; malleable signatures were introduced and explained to the participants since they lack the technical knowledge to argue or discuss

functionalities. The focus was rather on general problems and requirements of signature schemes. Consequently, specific requirements of (subsections 4.3, 4.4, 4.5) were mainly acquired from participants of the focus groups because these participants were able to relate and discuss malleable signatures in depth with regards to the eHealth use case. Focus group discussions were detailed in regards to malleable signatures creation and redaction rules. Results were mainly describing functionality, responsibility, accountability, and usability requirements of malleable signatures.

4.1. General Requirements for the Hospital Platform

The interviews with eHealth specialists showed that in practice for simplicity a group login instead of personal logins to personal accounts is used for health care professionals such as nurses. As a consequence, it is not traceable who did what actions in regard to medical records, i.e. the respective users cannot be made accountable. Thus, a fundamental requirement for a system in e-Health is RH3: Personal login is required for personal accountability as a means for enhancing patients' trust in the overall eHealth system. However, also when personal login is required, interviews reported that personal accountability was often "obfuscated" by staff neglecting to logout and login for reasons of convenience – people rather prefer to trust their colleagues than to struggle with repeated login activities. Personal login and correct user authentication are however not only essential for accountability and user's trust of the system, but also a prerequisite for the correct functioning of electronic signature schemes in general. At one of the healthcare organisation interviews, currently medical documents can be non-electronically "signed" by simply changing the status of a document as "signed", and there have already been incidences where user operating on the account of another user have mistakenly signed a document under the other user's identity. Hence, users need to be convinced and motivated to properly login and logout. Therefore, RH1 demands authentication to be secure and unobtrusive, e.g., by using a two-factor authentication scheme involving unobtrusive biometrics. Moreover, it was discussed that a system fulfilling RH2, that is providing functional benefits from logout/login, makes it easy for a user to motivate herself to actually logout when moving from one computer to the next because she will carry her session with her with all the data and applications open when she logs on to the next system.

There are more important means to increase the accountability that were mentioned in the interviews and are also mandated by the Swedish Patient Act, including transparency logging and providing patients with access to the logs referring to them (RH16), which could prevent staff from peeping (RH12) – especially, if recurrent updates to staff is given about of how many patients accessed the log data during a certain period.

4.2. General Requirements for the Cloud Portal

A prerequisite for the user adoption is that the user can establish reliable trust in the eHealth system including trust in the Cloud Portal, on which the patients can access,

redact and grant access to their medical data to other stakeholders, such as their private doctors or employers. Accountability and transparency means and controls that were discussed in our interviews as important instruments for enhancing trust (which is also the finding of Lacohée et al., 2006). Important accountability and transparency controls include usable privacy policy notices by the Cloud provides making their data handling practices including storage locations and applicable jurisdictions transparent (RG1), IT incident detection and reporting by the Cloud provider (RH7 & RH8). However, transparency & accountability controls that only leads to alarms will not build trust, and hence in addition to incidents reporting, cloud users also need means to put the right scope to any distrust they feel about Cloud solutions to check the trustworthiness of Health Cloud Portal. The interviews conducted revealed that in Sweden there is in general a high trust in solutions by the Swedish government (which is also confirmed by the findings of (Eurobarometer 2015)). "Health Care personnel have full trust in *Landstinget* (county council in Sweden) as an organization, therefore also in its functions, operations, and system." (Notes from an interview with a nurse.). Hence, the use of a private cloud run by the health authorities (e.g., *Landstinget*) (RH9) with a clear branding of the system owner (RH6) were elicited as requirements for helping users to develop reliable trust. Finally, easy-to use multi-factor authentication (RH1) is not only important for securing the patient's data against unauthorised accesses, but also contributes to the perception of security controls, which is also an additional factor contributing to the user's trust (Angulo et al. 2013).

4.3. Requirements for Malleable Signatures Creation

In our eHealth scenario, the doctor is defining the redactable fields of a patient's document and then creating a malleable signatures on that document in the hospital platform, before the document gets exported to the Cloud Portal. It was noted in the focus groups that it is crucial that the doctor's responsibilities for defining the permissible redactions must be clearly defined and understood (RH11), as these decisions can impact both the patient's privacy and safety. In this context, it was also discussed that there is a need for redaction policies (e.g., by using a formal specification language), which allow to clearly define what fields should be redactable in dependence on the data recipients and purpose of use (RF3B). Default redaction policy settings should be defined for different contexts, which are considering both data minimisation and the patient's safety (R1FG, RF3A). For example, if the recipient of the redacted patient document should be the patient's employer for the purpose of allowing the patient to prove that she was on sick leave at that hospital for a certain period of time, then all medical data should be set as redactable (or even marked as to be redacted by default by the patient's system). If however, the recipient should be another medical clinic, the redaction of information about the patient's medication could result in a bad drug-drug interactions thus jeopardizing patients' safety, and therefore should not be redactable.

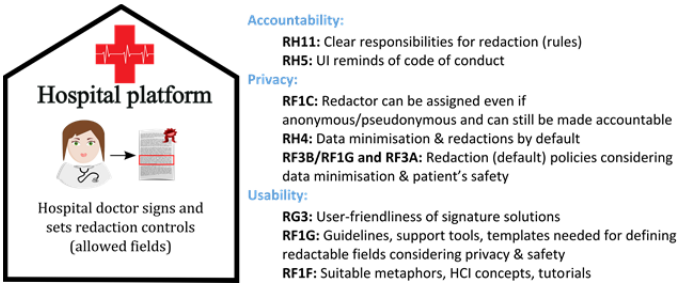

Figure 3: Requirements for malleable signatures creation in the Hospital Platform

If the signer who is in charge of sampling the blood test creates a malleable signature on the blood test which authorizes the patient concerned to do redactions on his blood test, then the identity of the patient may leak to the signer. However, for privacy reasons it is the practice that blood tests should be submitted anonymously. Hence, even if the redactor can be made accountable, there should be a possibility that the redactor can be anonymous or pseudonymous to the signer (so that the anonymity of blood tests can be guaranteed) (RF1C). In addition to redaction policies and usable templates defining redactable fields based on default policy settings, usable guidelines, tutorials and support tools are needed for informing users about how much information is advisable to redact for different use cases taking both privacy and patient safety criteria into consideration (RH4). Tutorials for understanding and using malleable signatures as well as for setting redaction rules, can help to mitigate misunderstandings, avoid unapproved redactions, and illustrate the implications and responsibilities of specific redactions (RH5, RG3, R1FG, and RF1F).

4.4. Requirements for Redactions of Signed Documents

Malleable signatures allow users to perform redactions, which was well acknowledged by the focus groups discussions as a privacy-enhancing feature giving the patient more control over their data. However, when the patient is redacting their medical document, they need to be aware of their responsibilities and the implications of redactions (RH11). Redactors should be accountable (i.e., the redactions should be "keyed" operations) (RF1B/RF1C) for the following reasons: If the redactor cannot be authenticated (i.e., if the redaction operation is "unkeyed"), the verifier may lack trust in the redaction, e.g. may not be sure that really only information that was not needed in a certain context was redacted by authorized persons. Moreover, the patient may repudiate. There should be clear redaction rules specified for the patient (RF3A, RF3B) for helping the patient to do redactions in different contexts taking the trade-off between privacy and safety into consideration, as well as default templates suggesting/enforcing default redaction settings for different use cases (RF1E). The patients may, however, not feel competent enough to do redactions themselves.

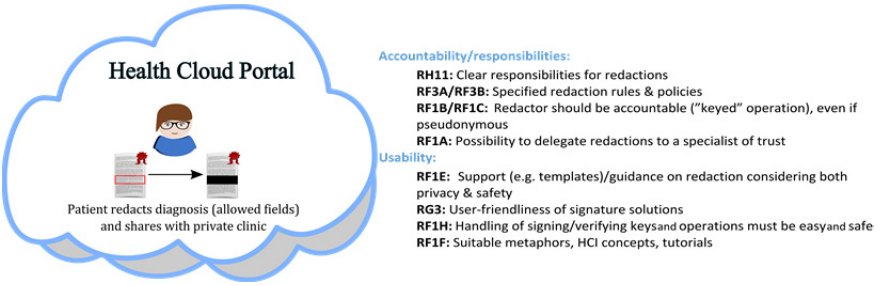

Figure 4: Requirements for Redaction of Signed Documents at the Cloud Portal

Therefore, there should exist RF1A: a possibility to delegate redactions to a specialist of trust. Moreover, the handling of signing/and verification keys and operations should be made easy and safe (RF1H). In one interview, it was noted how important it is to provide a representation of digital signature as a hand written image, when users found it difficult to comprehend digital signatures. However in this case, it becomes a concern when users depend on such representation (the image of handwritten signature) and end up in a situation where they trust a document with forged image signature without a digital signature. Therefore, it is important to choose suitable metaphors for the representation of signatures (RF1F).

4.5. Requirements for Accessing Redacted Documents

As one objective is not to burden the user with functional details and processes, a significant effort should be put into making the user interface as intuitive, simple, and user friendly as possible (RG3, RF1H, and RF5A). This is done by taking into consideration RF1F: suitable metaphors and HCI concepts to facilitate target functions of the solution for the Cloud Portal users, e.g., representation of the fact that a document is verified should be obvious and easily understood at the same time the invalidity of unverified documents should be clear. Suitable metaphors are also important for the user interface illustrations of redactions. Our former usability studies revealed for instance that in the context of anonymous credentials the "blacking out" metaphor that we used in the figures of this paper, were misunderstood by several test users as representing hidden or encrypted data rather than redacted data (Wästlund et al. 2012).

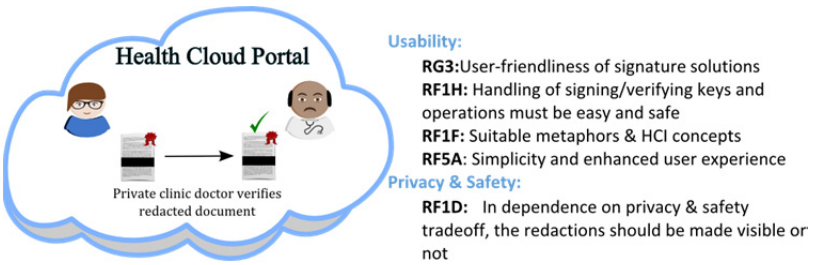

Figure 5: Requirements for Accessing Redacted Documents in the Health Portal

The focus groups were in particular also discussing questions around the representations of redactions, and whether redactions should be made visible or not. It may affect trust if the verifiers cannot distinguish the cases when data has been redacted from documents or not. On the other hand, privacy may be affected if the fact that information has been redacted (i.e. that the patient chose to hide certain medical values) cannot be hidden. If the "blacking-out" metaphor is used, meta-data could be derived easily from the illustrations (amount of data omitted is equivalent to the amount of space that has black ink on) and thus is discouraged. However, for the sake of the patient's safety, it might be important in certain cases to show that certain fields were redacted (e.g., on medical treatment). Therefore, in dependence on the use case, the redaction should be made "visible" or "invisible" to the verifiers, i.e. in some cases the very fact that data was redacted should be hidden (RF1D).

5. Conclusions

This paper evaluates the requirements that we elicited from stakeholders in regards to malleable signatures of the Cloud-based eHealth case scenario. The elicited requirements from their perspectives have shown that there is a need for clear definitions of roles and responsibilities of redactions. They should be supported by the functions and implementation of malleable signatures as well as suitable redaction policies and rules. Communicating these functions and policies, however, to users poses the greatest challenge. A conclusion is that the focus should be shifted from making users understand the inner workings of a tool towards adopting the use of the trusted tool and having an abstract (but justified) sense of security and privacy. Future work will aim for decreasing the burden on the user when the system is communicating information regarding the processes and functions of malleable signatures. Therefore we argue for an intuitive user interface supported by templates and default privacy-friendly settings. The user interface would require suitable metaphors to address users' intuitive mental models for trust and use. We aim to achieve that by continuing to follow UCD approach by developing the metaphors with mock ups for the user interface and further user interface testing.

6. Acknowledgement

This work received funding from the EU Horizon 2020 RIA programme under grant agreement No 644962 (PRISMACLOUD project).

7. References

Alaqra, A., et al., "Legal, Social, and HCI Requirements (Deliverable D 2.1)" PRISMACLOUD Project. To be published in 2016.

Alaqra, A., Fischer-Hübner, S., Gross, T., Lorünser, T., Slamanig, D., 2016. Trust and Accountability in the Cloud: Applications and Requirements. Proceedings of the IFIP Summer School on Privacy and Identity Management – Time for a Revolution? Springer 2016.

Angulo, J., Fischer-Hübner, S., and Pettersson, J., "General HCI principles and guidelines for accountability and transparency in the cloud (Deliverable D:C-7.1)," A4Cloud Project, 2013.

D. Demirel, D. Derler, C. Hanser, H. Pöhls, D. Slamanig and G. Traverso, PRISMACLOUD D4.4: Overview of Functional and Malleable Signature Schemes, 2015.

Eurobarometer, (2015). Data Protection Report. June 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Joinson, A.N., U.-D. Reips, T. Buchanan and C. Paine Schfield, "Privacy, trust, and selfdisclosure online," Human–Computer Interaction, vol. 25, no. 1, p. 1–24, 2010.

Khan, A.N., Mat Kiah, M.L., Khan, S.U., Madani, S.A., 2013. Towards secure mobile cloud computing: A survey. Future Gener. Comput. Syst., Special section: Hybrid Cloud Computing 29, 1278–1299. doi:10.1016/j.future.2012.08.003

Lacohée, H., Crane, S., Phippen, A., 2006. Trustguide: final report. Trust. Oct. 1, 25.

Schaar, P., 2010. Privacy by Design. Identity Inf. Soc. 3, 267–274. doi:10.1007/s12394-010-0055-x

Subashini, S., Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 34, 1–11. doi:10.1016/j.jnca.2010.07.006

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., Vasilakos, A.V., 2014. Security and privacy for storage and computation in cloud computing. Inf. Sci. 258, 371–386. doi:10.1016/j.ins.2013.04.028