Secure Storing of E-Health Records in the Cloud

Fabian Wiedemann(✉) and Martin Gaedke

Technische Universität Chemnitz, Chemnitz, Germany
{fabian.wiedemann,martin.gaedke}@informatik.tu-chemnitz.de

Abstract. Storing business sensitive data in the cloud is a huge challenge. Since disclosures of Edward Snowden, the trust in encryptions of the cloud provider decreased enormously. While this problem exists in many domains, like financial data, we identified a scenario in the e-Health sector. It is an important issue to preserve the patients' privacy when storing their e-Health records in the cloud. That is, encryption and decryption must be done by the client and it must be ensured that the cloud provider cannot access any e-Health record. Since a lot of e-Health records can be stored in such a system, it must be possible to search on the encrypted data without revealing any meta data or the records themselves. In this paper we present our planned research to securely store data in the cloud. We propose a first approach to deal with the identified requirements and describe our research methodology.

Keywords: Cloud · Security · Privacy · Encryption · Storage

1 Introduction

Over the last three years the usage of cloud computing by companies significantly increased [2]. Also, the revenue through cloud computing will grow within the next years by at least 15% annual [2]. On the one hand, important benefits why companies employ cloud computing are cost reduction in maintenance for software and infrastructure, higher scalability, and faster deployment of new software. On the other hand, a lot of companies in Germany hesitate to introduce cloud computing in their infrastructure. This is because they fear unauthorized access to sensitive business data [6].

One of the key issues companies need to deal with when using cloud computing is the privacy while storing personal data or business sensitive data in the cloud. Since the revelation of Edward Snowden, the trust in cloud providers regarding privacy issues decreased. While cloud providers encrypt the personal data or business sensitive data on the physical devices, they have the ability to decrypt the data and reveal them to others, like companies or official institutions, or process the data by their own. This is a huge obstacle for companies in using cloud computing, especially in sectors where privacy is important, like e-Health records or finance data.

P. Cimiano et al. (Eds.): ICWE 2015, LNCS 9114, pp. 635–638, 2015.
DOI: 10.1007/978-3-319-19890-3_46

We identified a scenario for storing e-Health records of patients in Germany in the cloud. The issue of privacy for the patient's e-Health records in Germany is regulated by a lot of laws and directives. To deal with these laws and directives special requirements need to be fulfilled by the software and cloud infrastructure.

2 Problem Analysis

Based on the described scenario of e-Health in Section 1, we analyze the following problem: Current cloud providers do not offer a secure and privacy-aware storage that fits legal requirements to store personal data, such as patient's e-Health records. In this context, we understand as secure and privacy-aware that the cloud provider will never have the ability to decrypt or reveal any information of the stored data.

The goal of our research is an approach that enables end users to securely store their personal data or business sensitive data in the cloud. For achieving the goal, we want to create a framework that supports web engineers to develop web applications that store their data in the cloud. The framework should consider privacy issues of the stored data and should never reveal any unencrypted data to third parties. To enable a wide usage of the framework, this needs to be applicable for any cloud provider.

3 Related Work

Literature to encryption partially deals with search-able encryption schemes. Bellare et al. in [1] and Song et al. in [4] focus on an encryption scheme which is secure against common attacks, while offering an efficient search on encrypted keywords. They propose an approach of a public-key encryption scheme that provides a deterministic encryption algorithm. That is, encrypting the same plain text, for example a keyword, two times with the same encryption key results in the same cipher text. Thus, searching on the encrypted keywords will provide the same results as searching on the plain keywords.

Besides the security topic in this research there is also related work in the context of software engineering. In [5] Vitali et al. describe an approach to build an e-Health infrastructure on the web. While our approach focuses on a client side encryption and storing only encrypted data, Vitali et al. developed a RESTful service to communicate e-Health records between medical practices, patients, and hospitals. Based on their recent work they evolved the framework SOLE to a REST architecture to reduce the overhead required by the previous one that uses SOAP for transmitting messages.

4 Approach

To deal with the problem described in Section 2, we propose a two-stage approach for secure storing documents in the cloud. One stage realizes the secure storing

of the documents in the cloud (cf. Figure 1 (a)), while the other stage utilizes the requesting of the documents from the cloud (cf. Figure 1 (b)). Our approach works as follows.

First, the client extracts keywords from the documents that should be stored in the cloud (cf. ①). As keywords we understand anything that is related to the document, such as often used words as well as meta data. Afterwards, the client encrypts the documents and the keyword-file-table (cf. ②). The key used for encryption is only stored on the client and does not have to be revealed to the framework or the cloud. Both, the encrypted documents and the encrypted keyword-file-table are sent to the framework (cf. ③). The framework stores the encrypted keyword-file-table for an efficient lookup performed during a search request. The encrypted documents will be stored in the cloud (cf. ④).

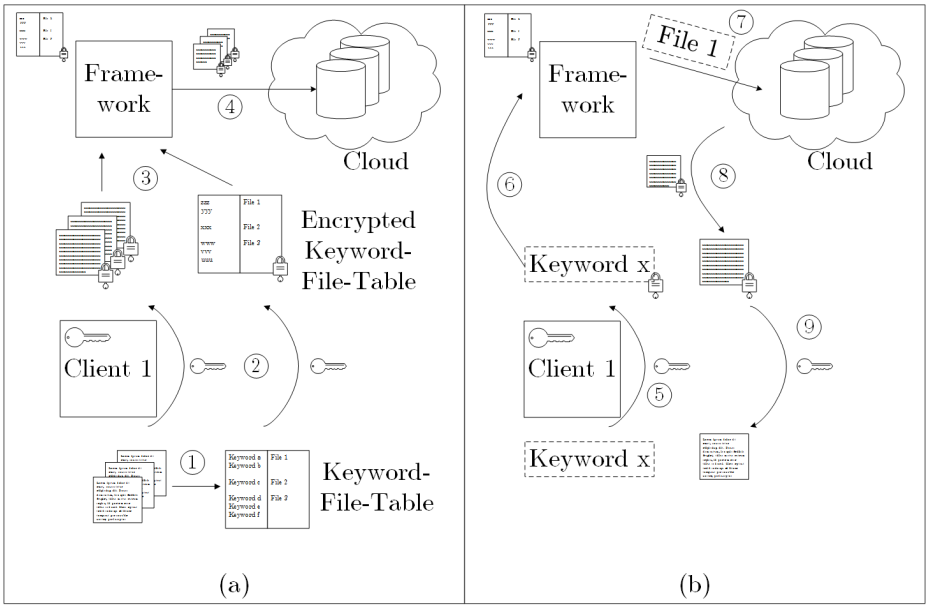

Fig. 1. Architecture of the approach

When the client wants to request a document to a specific keyword, the client encrypts the keyword using its stored key (cf. ⑤). The encrypted keyword is sent to the framework (cf. ⑥) and the framework can compute which document is requested based on the encrypted keyword-file-table. Afterwards, the framework requests the encrypted document from the cloud (cf. ⑦). The framework receives the encrypted document from the cloud and sends it to the client (cf. ⑧). In the last step, the client decrypts the encrypted document with its stored key and can process the document (cf. ⑨).

5 The Research Methodology

The research proposed in this paper will be structured following the Logical Framework Approach (LFA) [3]. LFA covers three stages of our research, i.e., identification, formulation, and evaluation. In the first stage, we identified the stakeholders of the proposed problem, i.e., doctors, nurses, patients, developers, and cloud providers. By interviewing and surveying these stakeholders we want to capture and analyze their problems. Based on the analyzed problems we derive objectives our approach needs to achieve. Within the formulation stage, we create measurable outcomes and define the scope of our research. Independently from LFA, we implement our approach between formulation and evaluation stage. In the last stage, we evaluate and measure how our objectives are fulfilled.

6 Conclusions

This paper presents an approach for a framework to securely store personal data and business sensitive data in the cloud. Based on a use case in the e-Health sector we analyze problems and challenges for the success of the proposed approach. We describe a first draft how we want to tackle the problems of a full client-side encryption and the challenge of a search-able encryption scheme.

Future work will focus on multiple user collaboration. That is, one user wants to invite another user to collaborate with him on an encrypted document in the cloud. Therefore, an easy to use and secure key management needs to be used.

References

1. Bellare, M., Boldyreva, A., O'Neill, A.: Deterministic and efficiently searchable encryption. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535–552. Springer, Heidelberg (2007)
2. Columbus, L.: Gartner predicts infrastructure services will accelerate cloud computing growth, February 2013. http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/ (last accessed 2015–02-05)
3. European Commission: Project Cycle Management Guidelines, vol. 1 (2004). http://ec.europa.eu/europeaid/multimedia/publications/documents/tools/europeaid_adm_pcm_guidelines_2004_en.pdf
4. Song, D.X., Wagner, D., Perrig, A.: Practical techniques for searches on encrypted data. In: 2000 IEEE Symposium on Security and Privacy (S&P 2000), pp. 44–55. IEEE (2000)
5. Vitali, F., Amoroso, A., Roccetti, M., Marfia, G.: Restful services for an innovative e-health infrastructure: a real case study. In: 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 188–193. IEEE (2014)
6. Wallraf, B.: Cloud-monitor 2014. Tech. rep., KPMG AG (2014)