PAL SAaaS - Building Triangular Trust for Secure Cloud Auditing

The most relevant security threats in cloud computing are data breaches and data loss. Thus, to bring cloud computing to the next level, customers need to be ensured that a cloud provider securely and transparently offers the promised functionality. The currently discussed and probably most promising concept is 'Security Adit as a Service' (SAaaS) where a third party, called the auditor, supervises the cloud provider on behalf of the user.

Therefore, the overall project is to develop and integrate cryptographic building blocks for secure and liable cloud audits. Our focus will be on **PAL** as the acronym for:

Privacy: The process of auditing requires the collection and analysis of digital evidence about the user and/or the service provider. It is necessary that by doing so, the privacy of these parties must not be violated. This also includes aspects like confidentiality of outsourced data.

Availability: A main concern with respect to the usage of cloud services is the availability of the outsourced data. Consequently, this needs to be also addressed by a cloud service audit. In addition, availability is necessary for the collected meta data and the results of computations as well.

Liability: This property has been mostly overlooked so far. Especially when cloud services are used by entreprises, the question of liability needs to be settled. This covers both the service provider and the auditor. In cryptographic terms: each party needs to be able to convincingly prove that it did its job.

The project will be coordinated by Universität Mannheim (UMA) and both partner will be involved into each task but partly to different extent. It is funded by the Baden Württemberg Stiftung up to an amount of €514,000 and will last from 11/2015 to 08/2018.

Projektmitarbeiter

Prof. Dr. Dirk Westhoff
M. Sc. Louis Tajan

Veröffentlichungen

L. Tajan, D. Westhoff, C. A. Reuter, and F. Armknecht. Private Information Retrieval and Searchable Encryption for Privacy-Preserving Multi-Client Cloud Auditing. In 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, Barcelona, Spain, December 5-7, 2016, pages 162-169. IEEE, 2016. http://dx.doi.org/10.1109/ICITST.2016.7856690

C. A. Gorke (Reuter), C. Janson, F. Armknecht, and C. Cid. Cloud storage le recoverability. In C. Wang and M. Kantarcioglu, editors, Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, SCC@AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2, 2017, pages 19-26. ACM, 2017.

L. Tajan, M. Kaumanns, D. Westhoff. Pre-Computing Appropriate Parameters: How to Accelerate Somewhat Homomorphic Encryption for Cloud Auditing, In 9th IFIP International Conference on New Technologies, Mobility & Security, February 2018. Paris, France