Université
franco-allemande
Deutsch-Französische
Hochschule

Activity Report

Armin Gerl

The processing of personal information is omnipresent in our data-driven society enabling personalized services, which are regulated by privacy policies. Although privacy policies are strictly defined by the General Data Protection Regulation (GDPR), no systematic mechanism is in place to enforce them. Especially if data is merged from several sources into a data-set with different privacy policies associated, the management and compliance to all privacy requirements is challenging during the processing of the data-set. Privacy policies can vary hereby due to different policies for each source or personalization of privacy policies by individual users. Thus, the risk for negligent or malicious processing of personal data due to defiance of privacy policies exists. In the thesis *'Modelling of a Privacy Language and Efficient Policy-based De-identification'* we propose a privacy-preserving framework.

My PhD proposes a solution to this problem by designing a Layered Privacy Language (LPL) which allows specifying legal privacy policies and privacy-preserving de-identification methods. Thus legal requirements and technical solutions are defined within LPL policies. Hereby, the formalization of privacy policies in an electronic format has many advantages for the management of privacy, because the privacy policy information is easily accessible, verifiable and structured. Thus, various Privacy Enhancing Technologies (PET) can be based upon LPL, i.e. user interfaces for consent management or Purpose-based Access Control (PBAC).

Furthermore, LPL policies are enforced by a Policy-based De-identification (PD) process, which enables the de-identfication of personal data according to LPL policies. This is an original contribution of the thesis. The PD process enables efficient compliance to various privacy policies simultaneously while applying pseudonymization, personal privacy anonymization and privacy models for de-identification of the data-set. Thus, the privacy requirements of each individual privacy policy are enforced filling the gap between legal privacy policies and their technical enforcement. Thus, handling of various individuals' privacy requirements can be handled, while business processes are not hindered.

The funds provided by the Deutsch-Französische Hochschule (DFH) / Universitè franco-allemande (UFA) supported the conduction of this thesis in a German-French context. This allowed an active exchange between Universität Passau and INSA Lyon. The financial support has been vital for the successful cotutelle PhD. The funds have been used to cover especially travel expenses between Germany and France, that otherwise could not have been provided.

The conduction and completion of the cotutelle PhD in the International Research & Innovation Center on Intelligent Digital Systems (IRIXYS) was an amazing experience as it fostered innovative research ideas due to the exchange of international research expertise as well as a great cultural exchange.