Distributed Privacy-Preserving Transparency Logging

Tobias Pulls
Department of Mathematics and Computer Science
Karlstad University
Karlstad, Sweden
tobias.pulls@kau.se

Abstract. We present a transparency-enhancing tool in the form of a cryptographic scheme that enables data processors to inform users about the actual data processing that takes place on their personal data. Our proposed solution can handle dynamic processes while offloading storage and interactions with users to dedicated log servers. On top of strong integrity and confidentiality properties, our scheme takes users’ privacy one step further by making it impossible to link multiple log entries for the same user or user identifiers across multiple data processors (for distributed processes). Our proposed solution has several applications, e.g., it can make access to electronic health records transparent to the patients to whom the records relate. Furthermore, we are the first to formalise the required security and privacy properties in this setting in a general manner (not specifically for our scheme) and prove that our scheme fulfils these. Finally, we show that our scheme is applicable in practice, providing performance results for a prototype implementation.

Fig. 1: Data processing is often distributed, where data disclosed by a user Alice may be shared by the initial data processor Bob with other data processors Charlie, Dave and Eve. Downstream data processing of Alice’s data should also be logged.