Encrypted Collaborative Real-Time Document Editing

K. Koerner, R. Finze, T. Walter

Chair of Information Services, University of Tuebingen, Waechterstrasse 76, 72074 Tuebingen, Germany

Collaborative real-time editors are used for parallel document editing across networks. Existing products as GoogleDrive\(^1\), Microsoft OneDrive\(^2\) or Etherpad\(^3\) require a trusted operation exchange server (OpES) which is responsible for storing persistent copies of the processed documents. Moreover the server synchronizes operations altering a document between all clients accessing it. The approach suffers from the fact that all clients have to trust the OpES since it has full access on the documents data. Therefore such a technique is not feasible for editing secret information. To solve this issue we researched a system architecture (see fig. 1) whose clients are responsible for ensuring the documents persistency. In this architecture the OpES is only trusted in building a proper sequence of operations and providing it to the clients through a web based interface. Thereby the documents and modifications content can be protected by encrypting the operations before storing them on the OpES. To retain the collaborative aspect of real-time document editing additional automated key exchange and identity management components are required and accessible for the involved clients. Since the OpES does not store a persistent copy of the document it is important to be aware of the transaction management ensuring all clients keeping a synchronized persistent document representation. Therefore we analysed common use cases and created workflow diagrams describing all tasks occurring in the transaction management (an example can be found in fig. 2). To validate our theoretical assumptions we implemented a prototype including a javascript client, a PHP based RESTful OpES component and PHP based components for identity and key exchange management. Currently we are reviewing this implementation relating to user experience, usability and performance to demonstrate the practical applicability of the researched approach.

Fig. 1 – System architecture providing encrypted collaborative real-time document editing.

Fig. 2 – Top level workflow including tasks required for handling a document modification on a single client.

---

1. https://www.google.com/drive/
2. https://onedrive.live.com