
- Master/Diploma thesis -

Secure Mobile Cloud Service for personal data with web frontend based on HTML5

CASED

In CASED (Center for Advanced Security Research Darmstadt) the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the Darmstadt University of Applied Sciences collaborate in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. Read more on www.cased.de.

Motivation & Goal

Today, personal data of users is distributed on a large variety of devices. Ranging from standard PCs and laptops, to cell phones, Smartphone and tablet PCs. The variety of devices makes it difficult for users to keep their data synchronized among all platforms. The current approach is to synchronize the mobile devices not among themselves but with a cloud service provider. Such synchronization is very convenient, but carries the risk that personal data may fall into the wrong hands, caused by the online service itself (e.g. vulnerabilities in the software) or a successful attack.

Using encryption on the user side could significantly reduce the risk of abuse, but with the drawback that web-based access is not working anymore. With the new features of HTML5 and JavaScript, this problem can be solved now. Goal of this work is to develop and implement a system that runs in the user's Web browser and automatically encrypts/decrypts the personal data stored on a server. This requires an evaluation of mechanisms for securely storing the key material on the client side. The resulting system should focus on ease of use while providing at the same time an acceptable security level for the user and his/her private data.

Requirements

- High motivation and capability to work independently
- Good knowledge on applied cryptography
- Knowledge HTML, JavaScript and AJAX
- Knowledge of client-server systems and network protocols such as HTTP is an advantage

Contact

If you are interested, please contact Jan Peter Stotz
EMail: jan-peter.stotz@sit.fraunhofer.de