



Adrian
Anthamatten



Peter
Frick



Jeyanthan
Ravindran

Diplomanden	Adrian Anthamatten, Peter Frick, Jeyanthan Ravindran
Examinator	Prof. Oliver Augenstein
Experte	Reto Bättig, m&f engineering, Fahrweid, ZH
Themengebiet	Internet-Technologien und -Anwendungen

Entwicklung eines WebDAV Proxy zum sicheren Speichern von Daten in der Cloud

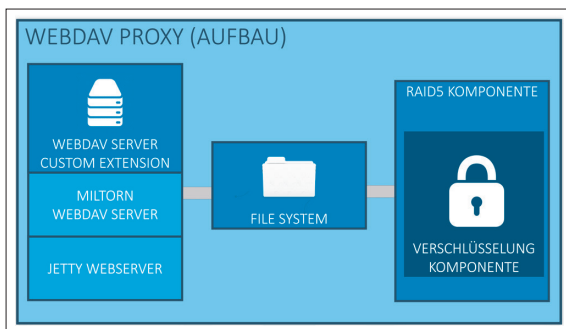
Evaluation und Erweiterung eines WebDAV Server



Mit dem Proxy-Server möchte man die Daten vor dem Zugriff der Cloud-Anbieter schützen.

Ausgangslage: Durch die stetig steigende Internet-Bandbreite und Verfügbarkeit mobiler Netze stehen neue technologische Möglichkeiten wie Cloud-Dienste zum Speichern von Daten zur Verfügung. Diese werden immer günstiger und damit auch attraktiver für die breite Masse. Solche Dienste haben aber oft auch gravierende Nachteile: In den letzten Jahren gab es immer wieder Berichte über Datendiebstähle, und es ist kein Geheimnis, dass vor allem preisgünstige Cloud-Anbieter die gespeicherten Daten für Auswertungen und Analyse Zwecke verwenden. Ausserdem garantieren die Anbieter bei kostenlosen Angeboten keinen Schutz vor Datenverlust.

Vorgehen/Technologien: Das Ziel dieses Projekts ist eine WebDAV-basierte Anwendung, die die Daten über mehrere Cloud-Anbieter redundant verteilt. Dadurch ist sichergestellt, dass Daten nicht verloren gehen, wenn ein Anbieter die Daten temporär oder dauerhaft nicht mehr zur Verfügung stellen kann. Des Weiteren sollen die Daten vor unerwünschten Zugriffen der Provider so geschützt werden, dass gängigen Cloud-Funktionen, wie z. B. das Teilen von Dokumenten, weiterhin genutzt werden können.



Der Proxy-Server konvertiert ein WebDAV-basiertes Filesystem für den Benutzer transparent in verschlüsselte RAID5-Datenblöcke.

Ergebnis: Das Resultat dieser Arbeit ist ein WebDAV Server, der als Proxy zwischen Client und Cloud-Anbieter fungiert. Sobald der Proxy-Server mit mehreren Cloud-Anbietern verbunden ist, kann sich der Benutzer über einen beliebigen WebDAV Client mit dem Proxy-Server verbinden und wie gewohnt seine Daten manipulieren. Die Daten werden für den Benutzer transparent nach dem RAID5-Verfahren in Blöcke aufgeteilt, die so auf die Provider verteilt werden, dass bei einem Ausfall eines Cloud-Anbieters weiterhin auf die Daten zugegriffen werden kann. Um den Zugriff der Provider auf die Daten zu verhindern, werden die bei den einzelnen Providern abgespeicherten Datenblöcke mit automatisch generierten Keys verschlüsselt. Diese Keys werden dann bei einem anderen der beteiligten Provider abgelegt, was gewährleistet, dass ein einzelner Provider die bei ihm gespeicherten Daten nicht entschlüsseln kann. Beim Lesen einer Datei sammelt sich der Proxy-Server alle relevanten Blöcke und entschlüsselt diese mit den dazugehörigen Keys. Um Daten mit anderen Benutzern zu teilen, können Links generiert und verschickt werden. Mithilfe dieser Links und einem eigenen Proxy-Server können die anderen Benutzer auf die freigegebenen Daten zugreifen.