

Sicherer und redundanter Cloud-Speicher SRCS

Fachgebiet: Verteilte Systeme und Sicherheit

Betreuer: Arnaldo Cremisini

Experte: Rolf Wenger

Industriepartner: Scherer Informatik GmbH, Siselen

Sicherer und redundanter Cloud-Speicher SRCS ist eine clientseitige und providerunabhängige Middleware, welche die heterogenen Schnittstellen von Cloud-Storage-Providern CSP adaptiert und mit kryptografischen Techniken in ein sicheres und redundantes Netzwerkdateisystem auf dem Datenspeicher der CSPs abbildet. Durch die offenen Schnittstellen und die Providerunabhängigkeit bietet die Lösung einen hohen Investitionsschutz. Die clientseitige strenge Verschlüsselung erlaubt selbst sensible Daten sicher und redundant in der Cloud zu speichern.

«Infrastructure as a Service», kurz IaaS, ist ein Teilbereich des Cloud Computings. IaaS im Allgemeinen und Cloud-Speicher z.B. für Datenbackups im Besonderen sind für kleine und mittelständische Unternehmen sehr attraktiv. Der Vorteil: Es müssen keine Investitionen getätigt und es muss kein oder nur geringes Know-how aufgebaut werden. Weiter bezahlt der Kunde immer nur den benötigten Speicherplatz, respektive die benötigten Ressourcen. Trotz den attraktiven Preisen gibt es bei vielen potentiellen Kunden Zurückhaltung, da es noch diverse Bedenken bezüglich Sicherheitsrisiken oder dem Datenschutz gibt. Die zentralen Fragen sind:

- Werden die Passwörter und Daten gesichert übertragen?
- Wie sieht es mit der Vertraulichkeit aus? Wie kann sichergestellt werden, dass die Daten in der Cloud nur berechnigte Personen einsehen können?
- Was passiert bei Vertragsende oder Konkurs des Anbieters mit den Daten?
- Wie sieht der Zugriff auf die Daten aus? Ist die Verfügbarkeit jederzeit gewährleistet?
- Ist den gesetzlichen Anforderungen bezüglich Personendaten genüge getan?

SRCS greift die oben skizzierte Problematik auf und hat folgende Zielsetzungen:

Es soll eine clientseitige providerunabhängige Middleware realisiert werden, welche einen sicheren und redundanten Zugriff und Ablage der Daten bei den Cloud-Storage-Providern ermöglicht. Dabei soll nicht die Standard-Software der einzelnen Anbieter verwendet werden, sondern eine eigene Software. Diese dient als Middleware, welche die eigentlichen Cloud-Services abstrahiert und direkt auf dem HTTP/REST-API der Provider aufsetzt. Damit wird Providerunabhängigkeit erreicht und die Interoperabilität gefördert.

Was ist SRCS im Detail

SRCS ist eine Middleware, welche einerseits mit protokoll- oder providerabhängigen Adaptern die Dienste der Cloud-Provider einbindet und andererseits die

Dienste providerunabhängig anderen Programmen zur Verfügung stellt. Im Kern der Middleware befindet sich der Crypto-Layer, welcher die Daten mit kryptografischen Algorithmen ver- und entschlüsselt. Die Service Provider SP stellen den eigentlichen Speicher zur Verfügung. Als SP kann ein konventioneller FTP-Server eingesetzt werden, ein Filesystem oder ein Cloud-Speicher-Anbieter wie Amazon S3, Google-Drive Google oder Skydrive von Microsoft. Die Service-Provider werden mit ihrem «native» Protokoll wie S3 oder über http(s), ftp etc. angesprochen. Pro unterstütztes Protokoll muss ein Service-Adapter implementiert werden.

Jeder Service-Adapter SA ist für ein unterstütztes Protokoll zuständig. Jeder Service-Adapter implementiert eine spezielle Schnittstelle, damit jeder Adapter auf die gleiche Art und Weise angesprochen werden kann. Der Transfer-Manager TM ist zuständig für die kontrollierte Übertragung der Daten.

Der Crypto-Layer beinhaltet alle kryptografischen Funktionen, welche für das Ver- und Entschlüsseln der Daten und Dateinamen, die Hashsummenberechnung, die Schlüsselableitungen und die Komprimierung der Daten gebraucht werden.

Der File-System-Layer bildet den obersten Layer und bildet alle benötigten Operationen eines klassischen Dateisystems ab und dient damit als Dienstschnitt für Applikationen.

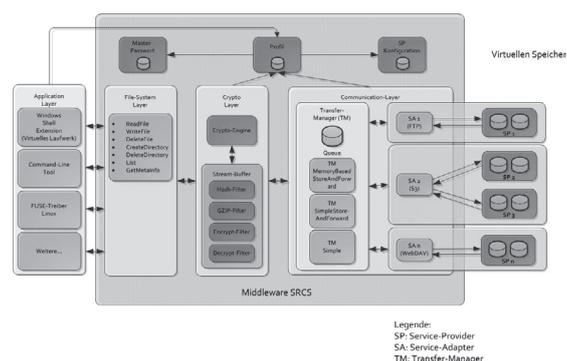


Rolf Scherer

+41 79 218 42 16

rs@scherer-informatik.ch

Architektur SRCS Middleware / Virtuelles Dateisystem



Architekturdiagramm