MimoSecco – Middleware for Mobile and Secure Cloud Computing


Gunther Schiefer


Matthias Gabel


Prof. Dr. Müller-Quade


Oliver Winzenried


Gerald Hübsch


Spiros Alexakis


Tamara Högler

Vertrauen ist gut – Kontrolle ist besser +++ Vertraulichkeit von Daten beim Cloud Computing +++ MimoSecco – Ein Forschungsprojekt der SaaS4KMU-Partner

Cloud Computing, eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen, hat in den letzten Jahren die IT-Landschaft grundlegend verändert. Die Bereitschaft, private oder Firmendaten in eine „Wolke" auszulagern, ist jedoch nicht so hoch wie von Analysten vorhergesagt. Insbesondere Sicherheitsbedenken werden als große Hürden für die Einführung von Cloud Computing in Deutschland genannt. Ansätze zur Reduzierung dieser Sicherheitsbedenken gibt es viele: Private Cloud, Deutsche Cloud usw. Damit wird aber die Grundidee des Cloud Computings aufgegeben, beliebige Ressourcen weltweit nutzen zu können. Mehrere Partner aus dem durch das CyberForum e.V. koordinierten SaaS4KMU-Konsortium haben sich deshalb zusammengeschlossen, um sich diesen Herausforderungen zu stellen. Im Rahmen des vom Bundesministerium für Wirtschaft und Technologie geförderten Projekts „MimoSecco" (Middleware for mobile and secure cloud computing) entwickeln sie eine Lösung, welche es Datenbesitzern ermöglichen soll, bei der Nutzung von mobilem Cloud Computing stets die Kontrolle über die Datennutzung zu behalten. Um das Angriffspotenzial bei eingeschränkt vertrauenswürdigen Cloud-Anbietern zu verringern, verfolgt MimoSecco das Konzept der Verschlüsselung und Speicherung der Daten bei organisatorisch und/oder räumlich getrennten nachgelagerten Cloud-Anbietern.

Insbesondere für Unternehmen spielt die Vertraulichkeit der Daten in der Cloud eine wichtige Rolle – nicht nur aufgrund gesetzlicher Vorschriften, sondern insbesondere aufgrund der hohen Sicherheitsansprüche ihrer Kunden. Erprobtes Mittel zur Sicherung der Vertraulichkeit ist eine konsequente und ausreichende Verschlüsselung der Daten bei Transport und Speicherung. Sollen diese Daten durch Dritte bearbeitet werden, müssen sie hingegen nach aktuellem Stand der Technik zumindest teilweise entschlüsselt vorliegen. Durch die hohe Konzentration der Daten vieler Unternehmen bei einem Anbieter ergeben sich hierdurch ganz neue Potenziale des Datenmissbrauchs. Insiderangriffe, also Angriffe durch Personen, welche berechtigten Zugang zu den Räumen, der Infrastruktur oder den IT-Systemen eines Cloud-Anbieters haben, müssen hier als ganz neues Problem betrachtet werden.
Im Architekturmodell von MimoSecco werden drei Sicherheitszonen unterschieden: Die berechtigten Nutzer der Daten beim Cloud-Anwender, der primäre Cloud-Anbieter (1st Level) und die nachgelagerten Cloud-Anbieter (2nd Level). Den berechtigten Nutzern in der linken Zone wird vollständig vertraut. Diese müssen über ein Sicherheitstoken verfügen; ohne diesen ist eine Nutzung der Daten nicht möglich. Die anschließende mittlere Zone stellt den eingeschränkt vertrauenswürdigen (primären) Cloud-Anbieter dar, zu dem ein direktes Vertragsverhältnis besteht. Dieser übernimmt die Funktion der Datenverteilung und -aggregation. Die Daten werden hier nicht persistent (d. h. auf Festplatte) gespeichert, sondern liegen immer nur bei Bedarf temporär im geschützten Speicher (RAM) vor. Diese Cloud-Anbieter werden hier als eingeschränkt vertrauenswürdig bezeichnet, da sich die Verarbeitung der

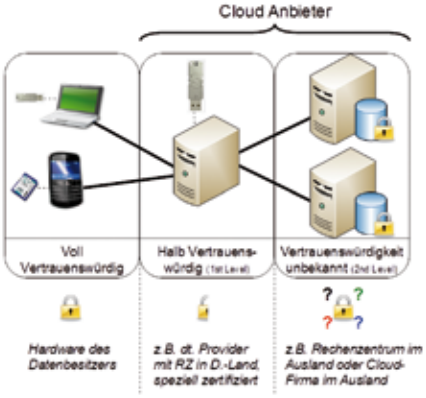

Abbildung 1: MimoSecco Zonenmodell

Daten nicht mehr im direkten Einflussbereich des Cloud-Anwenders befindet und neuartige Insiderangriffe denkbar sind. Diese Art von Cloud-Anbieter kann im Modell von MimoSecco auch der Betreiber von SaaS-oder PaaS-Diensten sein. Die nachgelagerten Cloud-Anbieter sind nicht direkt vertraglich mit dem Cloud-Anwender verbunden. Ihre Vertrauenswürdigkeit ist daher aus Sicht des Cloud-Anwenders unbekannt. Hier werden die Daten verschlüsselt bzw. Indizes teilverschlüsselt gespeichert.

Ein sicherer Datenbankadapter verschlüsselt die Daten und verteilt sie auf mehrere Cloud-Anbieter. Alle Operationen laufen automatisch und völlig transparent für den Benutzer ab. Dieser sichere Datenbankadapter wird in die offene Plattform CAS OPEN von CAS Software integriert und liefert eine vertrauenswürdige, verteilte Cloud Umgebung für mobiles CRM (Customer Relationship Management). Die Zugriffskontrolle basiert dabei auf „Kontextschaltern", welche die Zuordnung von Rechten an Daten zur Laufzeit abhängig von der aktuellen Situation des Anwenders festlegen. Der Nutzen der sicheren CAS OPEN Plattform wird mit der Umsetzung von zwei Referenzszenarien gemessen. Das Szenario technischer Kundendienst fokussiert auf den sicheren Aufbau, Betrieb und Wartung von Solaranlagen in Europa und Indien. Das Referenzszenario Beratung vergibt Lese- und Schreibrechte, abhängig von dem Ort in dem sich ein Berater befindet.

Ein zentrales Element von MimoSecco ist die Nutzung von Sicherheitstoken als hardwaregestützte Vertrauensanker zur Erhöhung der Sicherheit und deren Wahrnehmung. Es handelt sich hierbei um spezielle Smartcards, welche wichtige kryptografische Funktionen und Daten sicher kapseln können (im Projekt wird dazu die von WIBU-SYSTEMS AG entwickelte CodeMeter® Lösung verwendet, vgl. [cod]). Durch ihre besondere Bauweise sind die Token gegen physische Manipulationen geschützt, sodass auch mit Seitenkanalangriffen oder Microprobing auf den Token gespeicherte kryptografische Schlüssel nicht ausgelesen werden können. Zusätzlich kann die Nutzung der Sicherheitstoken durch ein Kennwort abgesichert werden. Ohne die Eingabe dieses Kennworts ist dann kein Zugriff auf die enthaltenen Schlüssel möglich. Dadurch besteht z. B. ein zusätzlicher Schutz, wenn die Token gestohlen werden.

Die Projektpartner CAS Software AG, WIBU-SYSTEMS AG und das Karlsruher Institut für Technologie (KIT) arbeiten im Projekt MimoSecco gemeinsam an der Umsetzung der vorgestellten Möglichkeiten. Das Projekt endet im März 2014.

Dieser Artikel ist eine Zusammenfassung aus http://www.aifb.kit.edu/web/Article3082.

[cod] http://www.wibu.com/de/codemeter.html

Kontakt:
KIT – Institut AIFB
Gunther.Schiefer@kit.edu

KIT – Institut EISS
matthias.gabel@kit.edu

WIBU-SYSTEMS AG
E-Mai: info@wibu.com

CAS Software AG
E-Mail: spiros.alexakis@cas.de / gerald.huebsch@cas.de

CyberForum e.V.
E-Mail: hoegler@cyberforum.de