Nutzerkontrollierte Datenhoheit in der Cloud*

Erweiterter Abstract

Stephan Groß und Marc Mosch
Technische Universität Dresden
Institut für Systemarchitektur
01062 Dresden
E-Mail: {stephan.gross, marc.mosch}@tu-dresden.de

1 Einleitung und Motivation

Die jüngsten Fortschritte bei der Virtualisierung von Speicher- und Rechenressourcen in Kombination mit serviceorientierten Architekturen und breitbandigen Netzzugängen haben zu einer Renaissance bereits bekannter Konzepte aus Bereichen wie Grid, Utility oder Autonomic Computing geführt. Unter dem Schlagwort *Cloud Computing* werden heute unterschiedlichste Formen des bedarfsgerechten und sofortigen Ad-hoc-Zugriffs auf hochskalierbare Computer-Ressourcen zusammengefasst. Diese Ressourcen werden zu Dienstleistungen abstrahiert. Das Dienstangebot reicht hierbei von Infrastruktur- über Plattform- bis hin zu Softwarediensten. Die (finanziellen) Vorteile dieses Outsourcing für den Nutzer liegen auf der Hand: Er spart kostspielige Ausgaben für die Beschaffung und Wartung möglicherweise nur teilweise ausgelasteter Hardware, ohne auf die damit verbundene Flexibilität verzichten zu müssen.

Dennoch gibt es begründete Vorbehalte gegen den Einsatz von Cloud Computing, etwa Bedenken hinsichtlich der Datensicherheit und der Compliance. So tritt der Nutzer eines Cloud-Dienstes die Datenhoheit faktisch an den jeweiligen Cloud-Provider ab. Bisherige Ansätze, sicherheitskritische Dienste in dedizierten Private oder Hybrid Clouds anzubieten versprechen hierfür nur bedingt Abhilfe, bedeuten sie doch gleichzeitig eine deutliche Einschränkung der Flexibilität und Skalierbarkeit. Gleiches gilt für die Einrichtung nationaler Clouds.

Erforderlich sind stattdessen technische Mechanismen, mit denen der Nutzer in die Lage versetzt wird, die Migration seiner Daten und Dienste in die und innerhalb der Cloud zu kontrollieren. Mit ihrer Hilfe soll er bei der Verwendung etablierter Sicherheitsmechanismen, wie etwa kryptografischer Verfahren, unterstützt werden, um die aus den reduzierten Wartungskosten resultierenden Kostenvorteile von Cloud-Lösungen nicht zu verlieren. Dabei müssen neben den Sicherheitsanforderungen des Nutzers auch seine individuelle Einschätzung der Vertrauenswürdigkeit von Cloud-Providern berücksichtigt werden.

Die Entwicklung solcher technischer Mechanismen und der ihnen zugrunde liegenden Methoden ist das Ziel der Nachwuchsforschergruppe FlexCloud. Die im einzelnen geplanten Beiträge werden im folgenden kurz vorgestellt.

* Die Nachwuchsforschergruppe FlexCloud wird unter der Projektnummer 080949277 mit Mitteln des Europäischen Fonds für regionale Entwicklung und des Europäischen Sozialfonds sowie des Freistaates Sachsen finanziert.

2 FlexCloud – Flexible Service-Architekturen für Cloud Computing

In der Nachwuchsforschergruppe FlexCloud wird an Methoden und Mechanismen zur Unterstützung der Entwicklung *flexibler* und *sicherer* Cloud-Anwendungen gearbeitet. Als Grundlage dient unsere in den vergangenen Jahren im Rahmen des BMWI-Projekts Theseus/TEXO entwickelte Service-Plattform SPACE (vgl. Spillner, J.; Schill, A.: The TECЛA Service Platform: Web Service Sharing based on Modular Platform Services. FIS - Future Internet Symposium, Berlin, Germany, September 2009).

Flexibilität bedeutet hierbei die explizite Berücksichtigung nicht-funktionaler Eigenschaften von Cloud-Diensten, inklusive der an sie gestellten Sicherheitsanforderungen. Diese sollen vom Dienstnutzer vorgegeben und ihre Einhaltung mit dem Dienstanbieter in Form sogenannter *Service Level Agreements (SLA)* bindend vereinbart werden. Zu diesem Zweck werden in FlexCloud Verfahren zur maschinenlesbaren Spezifikation sogenannter *Service Level Objectives (SLO)*, d. h. nicht-funktionaler und sicherheitsrelevanter Eigenschaften von Cloud-Diensten, entwickelt. Darauf aufbauend werden weitergehende Mechanismen zur Handhabung von Cloud-Diensten entwickelt. Einerseits zur (semi-)automatischen Auswahl geeigneter Service Provider sowie Aushandlung von SLAs und andererseits zur Ableitung konkreter Monitoring-Ziele, um die Verletzung von SLAs zu erkennen und entsprechende Reaktionen abzuleiten. Des weiteren sollen in FlexCloud Strategien und Verfahren entwickelt werden, die bei vernetzten Nutzern und Cloud-Providern vorhandenen Computer-Ressourcen dynamisch zu einem virtuellen „Cloud-Rechenzentrum“ zusammenzuschließen. Ziel ist es, den Cloud-Nutzer in die Lage zu versetzen, auf Basis zugesicherter und überprüfbarer Eigenschaften die für seine Bedürfnisse am besten geeigneten Angebote auszuwählen.

Der *Sicherheitsaspekt* wird in FlexCloud auf zwei Arten adressiert. Zum einen als wichtiger Teilbereich der gerade geschilderten Arbeiten. So sollen Sicherheitsanforderungen an einen Cloud-Dienst als SLO formuliert und im Rahmen der SLA-Behandlung verbindlich und nachvollziehbar durchgesetzt werden. Auch werfen die geplanten Arbeiten eigene Sicherheitsfragestellungen auf, beispielsweise bezüglich der Integrität der beim Cloud-Provider erhobenen Monitoring-Daten. Für deren Beantwortung sollen auf Basis einer Risikoabwägung adäquate Vorschläge erarbeitet werden. Schließlich sollen im Rahmen von FlexCloud neue Mechanismen konzipiert und entwickelt werden, mit deren Hilfe der Nutzer die Übertragung seiner Daten kontrollieren und gemäß seiner Sicherheitsinteressen steuern kann.

Die in den einzelnen Bereichen erzielten Ergebnisse sollen in einer quelloffenen Service-Plattform für Cloud-Anwendungen miteinander integriert werden. Deren Rahmenarchitektur ist in Abbildung 1 umrissen. Grundidee ist, die Cloud als Zusammenschluss der verschiedenen Geräte einer Sicherheitsdomäne zu betrachten. Dies können die Endgeräte eines individuellen Nutzers (Personal Cloud, Π-Cloud), die Systeme eines einzelnen Unternehmens (Private Cloud) oder eines Zusammenschlusses mehrerer Unternehmen bzw. Behörden sein (Community Cloud). Die Nutzung (und das Anbieten) externer Dienste durch eine solche Cloud wird durch die sogenannte Π-Box realisiert. Diese stellt hierfür eine Service-Plattform sowie eine Komponente zur Kontrolle des Daten- und Servicetransfers zwischen verschiedenen Clouds, das sogenannte Π-Gateway, bereit. Die Π-Box verfügt damit über die Funktionalität eines Service Brokers sowie einer Application Layer Firewall. Technisch wird sie selbst als Service gekapselt, kann also sowohl als physisches Gerät – etwa als erwei-

terter DSL-Router oder dedizierter Server – oder als virtuelle Systemumgebung in der Cloud betrieben werden.

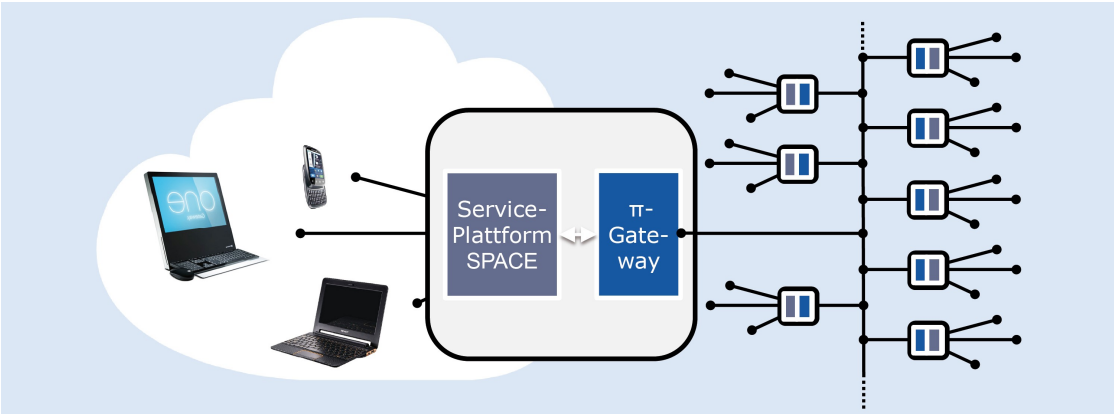

Abbildung 1: Architektur Π-Box

Zur weiteren Konsolidierung und Evaluierung soll die vorgeschlagene Lösung in typischen Anwendungsszenarien erprobt werden. Ein Beispiel hierfür ist die vertrauliche Speicherung von Daten in der Cloud. Zwar gibt es erste Lösungen, die eine nutzerseitige Verschlüsselung anbieten. Diese arbeiten jedoch losgelöst von bestehenden Zugriffskontrollsystemen und müssen manuell konfiguriert werden. Insbesondere sind die zugriffsberechtigten Nutzer respektive die verwendeten Schlüssel erneut festzulegen. Unser in Abbildung 2 skizzierter Lösungsansatz sieht vor, diesen Prozess durch Einbeziehung des Kontextes der zu speichernde Daten zu automatisieren. Das Π-Gateway greift hierfür beispielsweise auf Dateizugriffsrechte und die Nutzerverwaltung der Π-Cloud zu. Oder aber es führt eine Analyse der zu speichernden Daten durch. So könnten Verfahren zur Gesichtserkennung die dargestellten Personen auf einem Foto identifizieren, um gemeinsam mit den Kontaktdaten eines Nutzers deren öffentliche Schlüssel automatisch aus einer PKI zu extrahieren. Bei geschäftlichen und behördlichen Dokumenten ist die Informationsextraktion weniger aufwendig. Oftmals enthalten sie Anweisungen über den vorgesehenen Verteilerkreis, die sich mittels Methoden des Information Retrieval extrahieren und ebenfalls zur Konfiguration der notwendigen kryptografischen Operationen verwenden lassen.

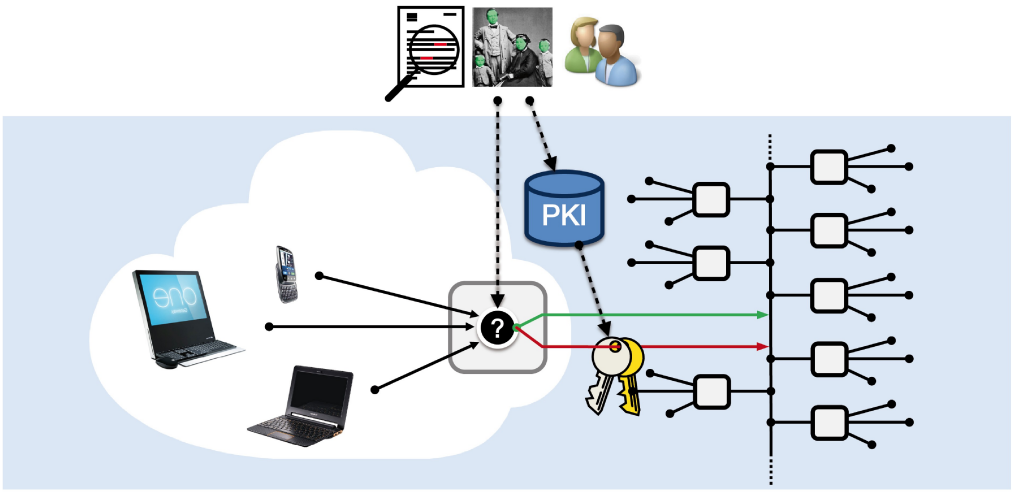

Abbildung 2: Automatischer Schutz der Vertraulichkeit durch die Π-Box