RAID in der Wolke

Bereitstellung sicherer und hochverfügbarer Speicherressourcen mit öffentlichen Clouds

Unternehmen haben hohe Erwartungen an das Cloud-Computing, aber auch große Bedenken bezüglich Sicherheit und Einhaltung gesetzlicher Vorgaben. Der vorliegende Beitrag stellt einen Lösungsansatz vor, um auch bei Cloud-Speichern Zuverlässigkeit zu gewährleisten und das Risiko abzuwenden, in eine Abhängigkeit von einem einzelnen Dienstleister zu geraten (Lock-in).

Von Maxim Schnjakin und Christoph Meinel, Potsdam

Die Beliebtheit und Relevanz von Cloud-Storage für Unternehmen hat in den letzten Jahren vermehrt zugenommen – die damit verbundenen Erwartungen sind vielfältig: bessere Skalierbarkeit, Kosteneinsparungen, Auslagerung nicht-wertschöpfender Aktivitäten und sicheres Vorhalten der Daten. Trotz wirtschaftlicher Vorteile zögern jedoch viele Unternehmen, interne Daten an externe Anbieter zu übertragen, besonders wenn es sich dabei um vertrauliche Daten wie Kundeninformationen, Buchhaltung oder juristische Dokumente handelt.

Dabei werden Diskussionen um Chancen und Risiken des Speicherns in der „Wolke" häufig zu pauschal geführt – denn Anbieter ist hier längst nicht gleich Anbieter. Eine Möglichkeit, verschiedene Cloud-Storage Provider (CSP) zu unterscheiden, ist diese in „Basic Storage Provider" (BSP) und „Advanced Storage Provider" (ASP) zu unterteilen [2]: BSPs betreiben eine eigene physische Infrastruktur zum Speichern der Daten. Üblicherweise bieten sie dem Endbenutzer keine grafische Oberfläche zum Zugriff, stattdessen können Daten über ein Application-Programming-Interface (API) programmatisch abgerufen werden. Zu den BSPs zählen unter anderem Amazon S3, Google Storage und Rackspace Cloud Files.

Im Gegensatz dazu betreiben ASPs keine eigene Infrastruktur zum Speichern der Daten, sondern greifen hierfür auf die Dienste der erwähnten BSPs zurück. Dafür bieten sie dem Endbenutzer in der Regel eine grafische Benutzeroberfläche zum Verwalten der Daten an, zum Beispiel als Desktopanwendung oder Web-Interface. Außerdem warten ASPs häufig mit Zusatzfunktionen auf, die über das reine Speichern von Daten hinausgehen. Dropbox ermöglicht etwa die Synchronisation ganzer Ordner über Rechnergrenzen hinweg. Weitere ASP-Beispiele sind Google Drive5 und Apples iCloud.

Herausforderungen und Probleme

Die Anzahl der Anbieter, die solche Dienste zur Verfügung stellen, hat sich in den letzten Jahren deutlich erhöht – laut [3] gab es bereits 2009 über 100 verschiedene Cloud-Speicher-Anbieter. Die Auswahl eines geeigneten Services ist für jeden potenziellen professionellen Nutzer sehr aufwändig – eine sorgfältige Prüfung ist unerlässlich, wobei eine individuelle „Due Diligence" höchst ineffizient ist. Als grundlegendes Szenario dient für den vorliegenden Beitrag ein deutsches Unternehmen, das seine – möglicherweise vertraulichen oder personenbezogenen – Daten in einer Public Cloud speichern möchte. Außer dem nachvollziehbaren Eigeninteresse, interne Informationsbestände vor Außenstehenden zu schützen, sind somit auch gesetzliche Vorschriften einschlägig, wie diese zu verarbeiten und zu verwalten sind (siehe etwa [4]).

Cloud-Anbieter versprechen zwar, für die anvertrauten Informationsbestände eine geschützte Umgebung zu liefern, doch die Verantwortung für den sicheren Umgang mit Daten liegt dennoch bei den Unternehmen, die den Dienst nutzen. Damit ist die Sicherheit im Cloud-Computing nicht nur eine Frage der Technik, sondern auch des Vertrauens. Denn einerseits müssen Dienstnutzer darauf vertrauen, dass Dienstanbieter ihre Daten vor Zugriffen unberechtigter Dritter ausreichend schützen. Andererseits müssen sie sich darauf verlassen, dass ihre Informationsbestände von Dienstanbietern nicht für eigene Zwecke missbraucht werden.

Darüber hinaus spielen Zuverlässigkeit und Verfügbarkeit bei externer Datenaufbewahrung eine wichtige Rolle: Beim Cloud-Computing werden Netzwerk-, Verarbeitungs- und Speicherfunktionen auf eine sehr große Basis physischer und virtueller Ressourcen ver-

teilt. Theoretisch soll dadurch eine wesentlich höhere Toleranz gegenüber einzelnen Hardware-Ausfällen erreicht werden – allerdings kam es auch bereits wiederholt zu aufsehenerregenden Ausfällen diverser Online-Speicherdienste.

Ein weiteres Problem tritt vor allem bei längerer Nutzung derselben Dienste auf und wird allgemein als Anbieter-Lock-in bezeichnet: Die Abhängigkeit der Nutzer wächst mit der Datenmenge, die an den externen Dienstleister übertragen wurde. Im Cloud-Computing verzichtet man zumeist auf langfristige Verträge – sollte ein Dienstanbieter von heute auf morgen seine Preispolitik ändern, können Kunden aber dennoch nicht ohne Weiteres zu einem anderen Anbieter wechseln: Auf der einen Seite ist ein Anbieterwechsel mit signifikanten Kosten allein für die Übertragung der Daten verbunden, da für den ausgehenden Datentransfer in der Regel seitens der Dienstleister Gebühren erhoben werden. So kostet die Migration eines 50 Terabyte großen Archivs beispielsweise von Rackspace nach Nirvanix rund 15.000 US-$. Auf der anderen Seite müssen meist bestehende Anwendungen an die Schnittstellen neuer Anbieter angepasst werden, da jeder Provider seine Dienste über proprietäre APIs bereitstellt, welche ihren eigenen Besonderheiten und Einschränkungen unterliegen. Ferner gibt es auch keine Garantie, dass der neue Dienstleister seine Preisstruktur dauerhaft beibehält.

Lösungsansatz

In einer Forschungsarbeit am Hasso-Plattner-Institut wurden ausgewählte Cloud-Speicheranbieter in einer einheitlichen Plattform integriert – hierzu dient eine Metaebene zwischen Anwendern und Cloud-Speicherdiensten. Zum besseren Schutz der Inhalte werden dabei einzelne Datenobjekte vor ihrer Übermittlung fragmentiert und verschlüsselt, die Fragmente anschließend unter Einhaltung nutzerspezifischer Anforderungen auf verschiedene, voneinander unabhängige Dienste verteilt.

Das System überprüft dabei die Einhaltung der Anwenderanforderungen und garantiert, dass kein Dienstanbieter im alleinigen Besitz der Anwenderdaten ist. Diese Verteilung erhöht nicht nur die Sicherheit und Zuverlässigkeit der Daten während der externen Aufbewahrung, sondern verringert auch deutlich die Gefahr des Anbieter Lock-ins: Denn im Falle einer Migration muss man nur einen Teil der Datensätze und nicht den gesamten Bestand übertragen.

Ziel des Forschungsprojekts: Ein Großteil des Entscheidungsprozesses zur Ermittlung geeigneter Dienstanbieter für die möglichst gleichmäßige Aufteilung der Nutzerdaten soll automatisiert erfolgen – ferner sollen Anwender ihre individuellen Anforderungen an das Hosting der eigenen Datenbestände festlegen können, ohne sich dabei um Administration und Leistungskontrolle kümmern zu müssen. Dieses Vorgehen für bessere Verfügbarkeit, Zuverlässigkeit und Sicherheit der Daten ist vergleichbar mit einer serviceorientierten Ausführung des RAID-Prinzips (Redundant Array of Independent Disks).

RAID-Systeme verbinden mehrere physische Festplatten zu einem logischen Laufwerk, um höhere Transfer- und geringere Ausfallraten zu erzielen – RAID-Systeme ab Level 2 nutzen eine Aufspaltung der Daten und verteilen einzelne Fragmente auf verschiedene Hardwareressourcen. Das Forschungsprojekt nutzt dasselbe Prinzip für Cloud-Speicher. Zur Aufteilung sowie Rekonstruktion der Daten werden Erasure-Coding-Techniken eingesetzt: Der große Vorteil liegt dabei in einem günstigen Verhältnis des Speicherbedarfs im Vergleich zur dazugewonnenen Datenverfügbarkeit. Der Ansatz ermöglicht der Meta-Plattform, den Ausfall eines oder so-

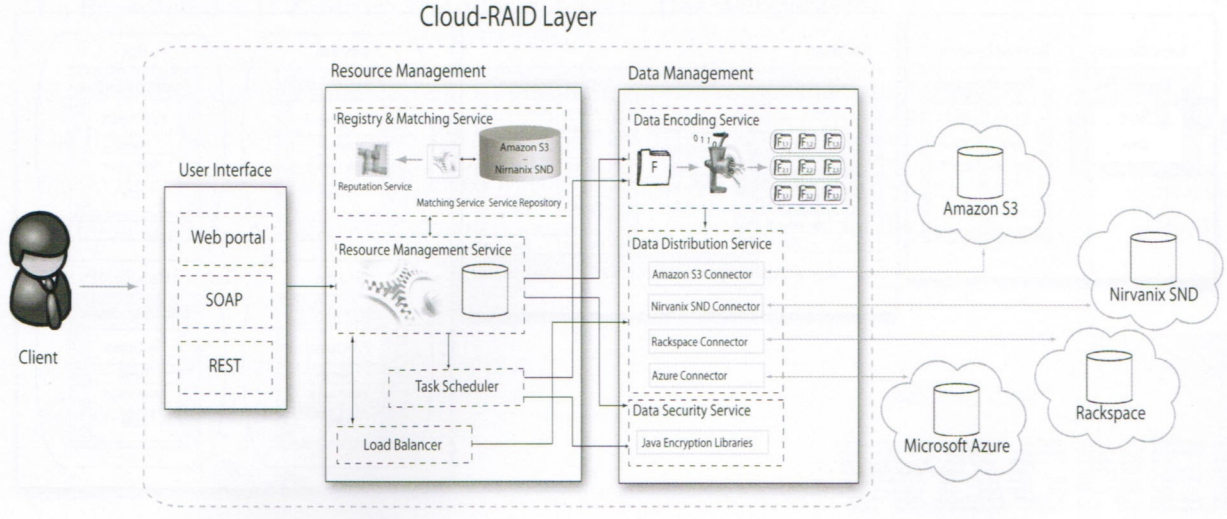


Abbildung 1: Grundlegende Architektur und Arbeitsweise der Cloud-RAID-Lösung.

gar mehrerer Online-Speicherdienste zu tolerieren, ohne Daten der Anwender zu verlieren – die Anzahl der tolerablen Ausfälle hängt dabei von den Anforderungen der Nutzer an die Verfügbarkeit der Daten ab.

Architektur

Die Cloud-RAID-Architektur besteht im Wesentlichen aus drei Komponenten:

Nutzer-Schnittstelle

Über diese Systemkomponente erhalten Anwender einen vollständigen Überblick über ihre Datenbestände sowie die verfügbaren technischen Features. Damit lassen sich Daten verwalten sowie Anforderungen an ihre Verwahrung festlegen (zum Beispiel in Form von Dienstleistungsparametern wie Verfügbarkeit, Reaktionszeit und Bandbreite). Es besteht die Möglichkeit neue Daten hochzuladen oder bestehende Inhalte zu verändern. Darüber hinaus können Anforderungen bezüglich der Sicherheit, geografischen Lage sowie Gebühren festgelegt werden.

Ressourcen-Management-(ResM)-Modul

Das ResM-Modul ist für eine „intelligente" Zuweisung von Daten an Cloud-Ressourcen verantwortlich und wird dabei von folgenden Diensten unterstützt:

- **Register- und Matching-Service:** bestimmt Cloud-Speicher-Provider basierend auf Nutzeranforderungen, überwacht die Leistung der Anbieter und stellt sicher, dass diese nicht gegen die Vereinbarungen verstoßen
- **Ressourcenmanagement-Service:** trifft alle operativen Entscheidungen bezüglich der Datenaufbewahrung sowie deren Verwaltung.

Zu Letzterem ist anzumerken, dass die Anforderungen Kosten, Verfügbarkeit und Übertragungsleistung nicht gleichzeitig „perfekt" erfüllbar sind: Höhere Verfügbarkeit erfordert beispielsweise eine Verteilung der Daten auf eine größere Zahl von Anbietern, was höhere Kosten nach sich zieht. An dieser Stelle müssen die Nutzeranforderungen gegen einen bestimmten Wert optimiert werden – zum Beispiel die beste Verfügbarkeit für einen vorgegebenen Grenzbetrag pro GB oder maximale Bandbreite für einen lesenden Zugriff unter Einhaltung eines bestimmten Verfügbarkeitswertes erreichen. Zur Ermittlung des optimalen Wertes wird die Lagrange'sche Multiplikationsmethode eingesetzt, bei der die einzelnen Anforderungen als Nebenbedingungen zusammengefasst werden.

Daten-Management-(DatM)-Modul:

Diese Komponente wird vom ResM-Modul angesteuert und ist für die physische Verteilung der Daten auf einzelne Cloud-Provider verantwortlich. Hierbei wird die Komponente von drei Diensten unterstützt: den Encoding-, Datenverteilungs- und Sicherheits-Services.

Der **Encoding-Service** ist für die Kodierung und Dekodierung einzelner Datenobjekte mittels Erasure-Algorithmen verantwortlich. Hierbei wird ein Datenobjekt in insgesamt $n=k+m$ Blöcke kodiert (Datenfragmente). Die Zahl n bezeichnet also die Anzahl der Datenblöcke, die nach dem Encoding entstehen und anschließend auf verschiedene, disjunkte Speicherquellen verteilt werden.

Diese Kodierung hat den Vorteil, dass jeder Datenblock mit k beliebigen Fragmenten (aus n möglichen) zu rekonstruieren ist [5]. Die Parameter m und k sind dabei frei wählbar. Der zusätzliche Speicherbedarf ergibt sich aus dem Verhältnis

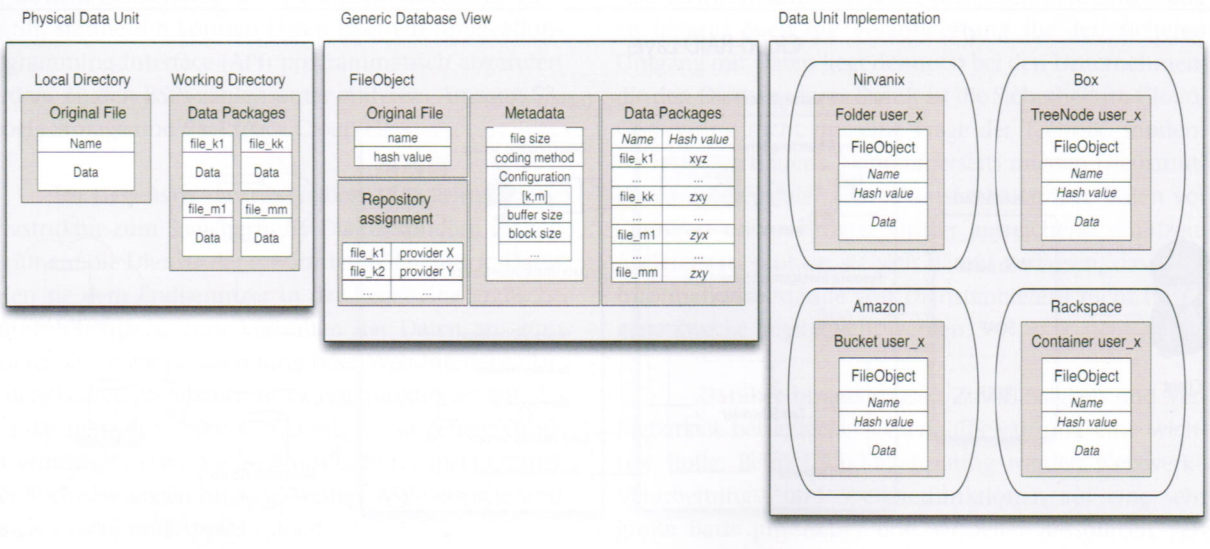


Abbildung 2: Das Datenmodell des Cloud-RAID-Systems

m/k: Bei Verteilung der Daten auf 11 Anbieter (mit einer exemplarischen Erasure-Konfiguration [10,1]) wäre das System in der Lage den Verlust von einer Quelle zu tolerieren. Der zusätzliche Speicherbedarf – der zusätzliche Kosten nach sich zieht – würde dabei 10 Prozent betragen.

Aktuell unterstützt das beschriebene System 12 Dienstleister, wobei die Ausdehnung der Funktionalität auf weitere Anbieter geplant ist. An dieser Stelle sei angemerkt, dass die eigentliche Kodierung der Datenobjekte sehr zügig erfolgt, sodass die dazu zusätzlich benötigte Zeit im gesamten Übertragungsprozess vernachlässigbar bleibt (vgl. Abb. 3): Der Kodierungsschritt nimmt in dem gezeigten Beispiel weniger als 0,5 % der gesamten Datenübertragung in Anspruch (die einzelnen Datenpakete wurden hierzu an folgende Anbieter übertragen: Google US, Amazon EU, Amazon (US-west-1), Nirvanix, Azure und Google EU).

Der **Datenverteilungsservice** verteilt die Fragmente anschließend auf verschiedene Speicheranbieter: Im Wesentlichen ähnelt das Datenmodell des Cloud-RAID (Abb. 2) dem von Amazon S3: Alle Datenobjekte werden in so genannten „Buckets" (Behälter) abgelegt. Jeder dieser Behälter besitzt einen eindeutigen Erkennungsschlüssel und wird systemweit nur ein Mal vergeben. Eine Schachtelung von Buckets ist nicht möglich. Ein Bucket kann beliebig viele Datenobjekte fassen, allerdings dürfen einzelne Objekte eine Gesamtgröße von 5 GB nicht überschreiten. Für jeden Anwender werden insgesamt *n* Speicherbehälter eingerichtet: Diese repräsentieren Buckets, die später auf verschiedene Cloud-Storage-Anbieter verteilt werden.

Die Kommunikation mit jedem einzelnen Provider findet über so genannte „Storage-Adapter" statt, welche die Funktionalität der eigentlichen Datenübertragung kapseln und die Kommunikation mit den proprietären Schnittstellen der Dienstanbieter vereinheitlichen. Die Adapter unterstützen grundlegende Funktionen zur Datenmodifikation (put, get, delete, list:object) und übersetzen diese in das jeweilige Format der Anbieter. Dieser Abstraktionsschritt kapselt somit die technische Komplexität im Umgang mit den proprietären Schnittstellen verschiedener Dienstanbieter und macht das System flexibel erweiterbar. Zur Ausdehnung der Funktionalität auf zusätzliche Dienstleister ist lediglich die Implementierung eines entsprechenden Adapters erforderlich.

Und schließlich ist der **Sicherheitsservice** für die Durchsetzung festgelegter Security-Richtlinien verantwortlich: Das initiale Sicherheitsniveau wird durch die physische Trennung der Inhalte gewährleistet, indem die ursprünglichen Datenobjekte auf unterschiedliche Cloud-Provider verteilt werden. Der Einsatz der Erasure-Algorithmen schließt das Durchsickern wichtiger Informationen jedoch nicht aus! Besonders wichtige Inhalte sollten daher verschlüsselt aufbewahrt werden.

Aus diesem Grund werden die Inhalte vor der Übertragung an Cloud-Anbieter verschlüsselt. Abbildung 3 zeigt deutlich, dass auch die hierfür benötigte Zeit im Vergleich zur eigentlichen Datenübertragung kaum ins Gewicht fällt. Daher sieht die Standardeinstellung vor, dass alle Daten vor der Übertragung verschlüsselt werden.

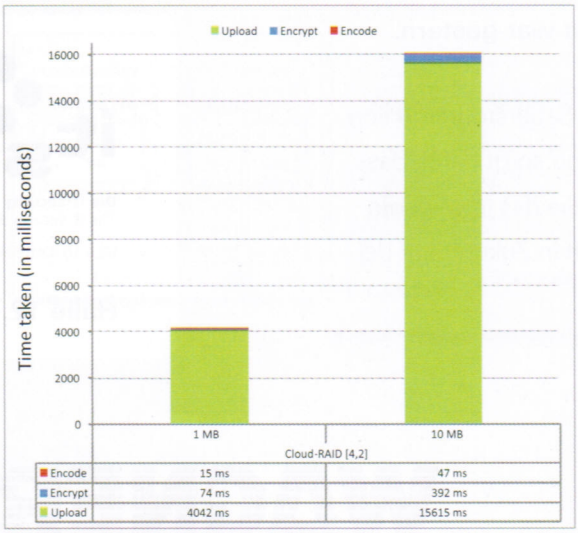
Beobachtungen und Ergebnisse

Zur Einschätzung der Leistungsfähigkeit des Forschungsansatzes wurde am Hasso Plattner Institut (HPI) ein umfassender Test der entwickelten Software durchgeführt, aus dem an dieser Stelle nur einige ausgewählte Ergebnisse vorgestellt werden können. Der Test lief insgesamt über mehr als 336 Stunden (ca. zwei Wochen) rund um die Uhr (7x24) – das Testbed umfasste sieben Cloud-Speicher-Anbieter mit verteilter Infrastruktur, sodass insgesamt 12 voneinander getrennte „Container" für das Cloud-RAID bereitstanden.

Da das HPI über eine Breitbandanbindung an das Internet (1Gb) verfügt, konnte sichergestellt werden, dass die Testsysteme selbst zu keinem Zeitpunkt einen Bandbreiten-Engpass während des Versuchs erfahren mussten. Die Gesamtdauer der Datenübertragung hängt von der Durchsatzfähigkeit der Anbieter ab, die in den jeweiligen Transferprozess einbezogen sind – der Test hat daher alle möglichen Konstellationen der Anbieter berücksichtigt, die das System zum aktuellen Zeitpunkt unterstützt.

Grundsätzlich kann der Einsatz von Erasure-Algorithmen die Leistungsfähigkeit der Datenübertragung gegenüber einer nativen Datenübertragung der gleichen Datei an einzelne Dienste deutlich erhöhen (vgl. [6]). Bei

Abbildung 3: Vergleich des Zeitaufwands für Kodierung und Verschlüsselung sowie Übertragung von Datenobjekten mit Cloud-RAID



einer genaueren Betrachtung der Ergebnisse fällt zudem auf, dass einige Anbieterkonstellationen wesentlich besser abschneiden als andere. Dieses Verhalten lässt sich damit erklären, dass die betrachteten Anbieter die Schnittstellen ihrer Dienste für bestimmte Anwendungsfälle optimiert haben.

In erster Linie fällt ein großer Unterschied in der Übertragungsleistung zwischen den Up- und Downloadfähigkeiten auch bei einzelnen Anbietern auf (vgl. Abb. 3): Nahezu alle getesteten Dienste zeigen im Download deutlich bessere Durchsatzwerte als im Upload – und zwar sowohl für die Übermittlung kleinerer als auch größerer Dateien. So kann beispielsweise der Schreibvorgang einer 100kB-Datei bei Google rund 12–19-mal länger dauern als ein lesender Zugriff.

Dieses Verhalten lässt sich auch bei der Übertragung größerer Dateien beobachten, wenn auch nicht mehr mit dermaßen drastischen Unterschieden: Aber auch hier unterscheidet sich die Performance um das vier- bis fünffache – mit Ausnahme des Anbieters Rackspace, bei dem ein Schreibzugriff sogar bis 49-mal langsamer ausfallen kann als ein Lesezugriff.

Andererseits ließ sich bei einzelnen Anbietern auch ein genereller Zusammenhang zwischen der Übertragungsleistung und der Datengröße beobachten: So erzielten bei der Übertragung kleinerer Dateien (bis 1 MB) Azure und Amazon EU (beim Upload) die besten Ergebnisse – bei 10 MB fällt Amazon EU bereits zurück. Ähnlich verhält sich auch Google US: Allerdings verbessern sich hier die Performancewerte mit wachsender Dateigröße – und zwar deutlich. Das beobachtete Verhalten kann damit zusammenhängen, dass die relativ große Reaktionszeit des Dienstes (welche in erster Linie auf die große Entfernung zwischen unserem Testsystem und dem Zielknoten zurückgeführt werden kann) bei größeren Dateien immer weniger die Messung der Übertragungsdauer beeinflusst.

Noch deutlicher lässt sich jedoch dieses Verhalten bei Google EU beobachten: Bei der Übertragung kleinerer Dateien zeigt der Dienst eine relativ schlechte Performance im direkten Vergleich zu den anderen Anbietern. Mit wachsender Dateigröße rückt der Dienst jedoch immer weiter nach vorne, bis er schließlich bei der Übertragung von 100 MB Dateien die Spitzenposition erreicht und damit den Dienst Azure ablöst.

Ähnliche Zusammenhänge ließen sich auch beim Downloadverhalten beobachten: Bei der Übertragung kleinerer Dateien, gehört Azure zu den führenden Diensten – mit wachsender Dateigröße fällt der Dienst jedoch immer weiter zurück. Auch Rackspace zeigt bei kleineren Dateien wesentlich bessere Performancewerte: Bei der Übertragung von Dateien mit einer Größe von 100 kB gehört er noch zu den führenden drei Anbietern – doch bereits bei einer Dateigröße von 500 kB fällt er auf den sechsten Platz zurück.

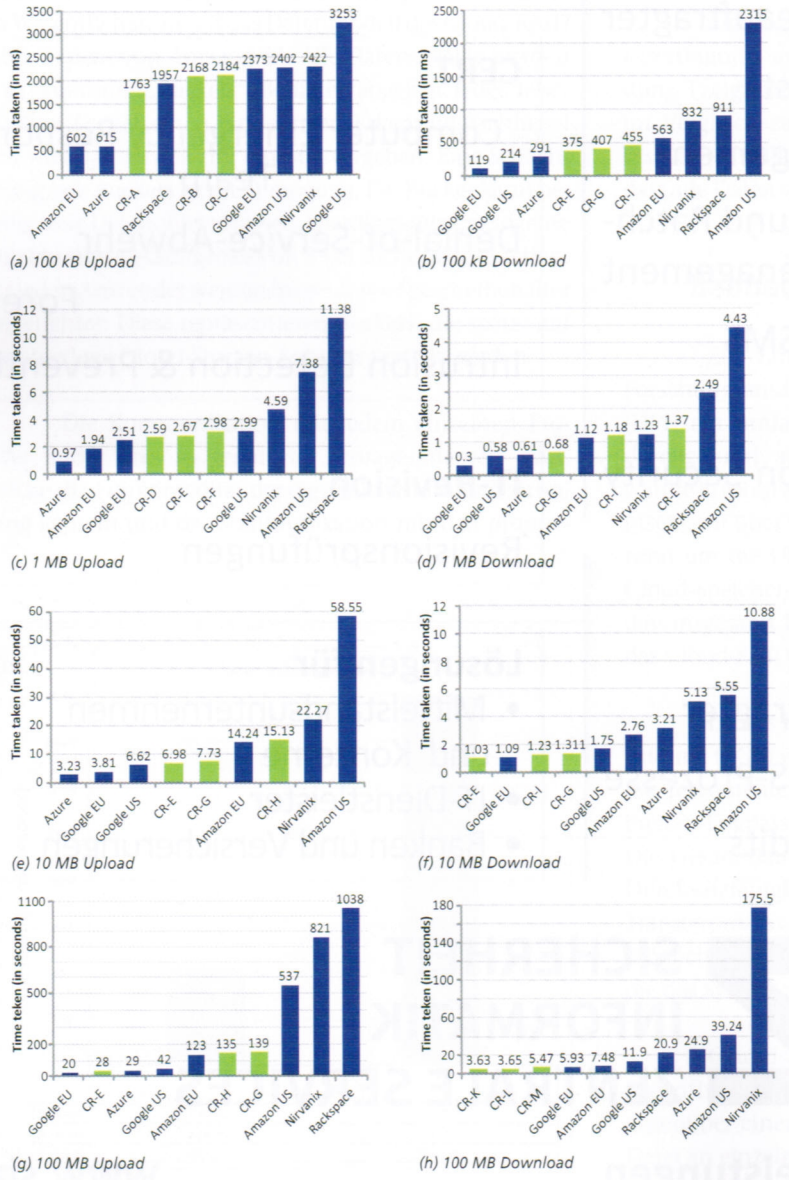


Abbildung 4: Vergleich zwischen Up- und Downloadgeschwindigkeiten bei verschiedenen Dateigrößen und Anbietern sowie im Cloud-RAID (CL) bei verschiedenen [4,1]-Konfiguration (Verteilung der Anwenderdaten auf insgesamt fünf Anbieter, wobei der Ausfall eines Dienstes toleriert werden kann)

Fazit

Das vorgestellte System schafft eine Metaebene zwischen Anwendern und Anbietern von Cloud-Speicherressourcen. Bei der Übertragung der Anwenderdaten werden die einzelnen Datensätze mittels Erasure-Codes fragmentiert und auf verschiedene, voneinander unabhängige Dienstleister verteilt – die hierbei beteiligten Cloud-Ressourcen können nach den benutzerdefinierten Anforderungen an Leistungsfähigkeit, geografische Lage sowie etwaige technische Eigenschaften ausgewählt werden.

Dabei wird sichergestellt, dass kein Anbieter in vollständigem Besitz der Anwenderdaten (aller zu einer einzelnen Datei gehörenden Fragmente) ist – zur Wiederherstellung der Originaldaten ist aber nur ein Teil aller Datenblöcke notwendig. Dieses Vorgehen erhöht einerseits die Zuverlässigkeit bei externer Datenlagerung und reduziert andererseits das Lock-in Risiko sowie die Gefahr eines möglichen Datenmissbrauchs seitens der Dienstleister.

Die Ergebnisse des durchgeführten Experiments zeigen deutlich, dass der Einsatz von Erasure-Codes – auch ohne zusätzliche Optimierung – ein gutes Verhältnis zwischen der Wirtschaftlichkeit und Effizienz für externe Datenlagerung bereitstellt (vgl. [6]). Darüber hinaus abstrahiert das System die technische Komplexität im Umgang mit den proprietären Schnittstellen verschiedener Dienstanbieter und ermöglicht seinen Nutzern einen einfachen Zugriff auf Cloud-Speicherressourcen.

Das beschriebene Forschungsprojekt ist vorerst abgeschlossen – die entstandene Software wird in Kürze frei verfügbar sein: Es ist geplant, den entsprechenden Client auf der Website des Hasso-Plattner-Instituts (HPI) zum Download bereitzustellen. Das System ist bereits seit einem Jahr im Einsatz und läuft stabil – dennoch ist anzumerken, dass es sich um eine prototypische Implementierung ohne Support handelt. ■

Dipl.-Inf. Maxim Schnjakin ist wissenschaftlicher Mitarbeiter am Hasso-Plattner-Instituts für Softwaresystemtechnik GmbH (HPI). Prof. Dr. Christoph Meinel ist Präsident und CEO des HPI und ordentlicher Professor für Informatik an der Universität Potsdam.

Literatur

[1] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology (NIST), NIST Special Publication 800-145, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Moritz Borgmann, Tobias Hahn, Michael Herfert, Thomas Kunz, Marcel Richter, Ursula Viebeg, Sven Vowé, On the Security of Cloud-Storage Services, SIT Technical Reports SIT-TR-2012-001, März 2012, www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf

[3] Toby Velte, Anthony Velte, Robert C. Elsenpeter, CloudComputing: A Practical Approach, McGraw-Hill, 2009, ISBN 978-0-07-162694-1

[4] Thomas Smedinghoff, Information Security Law: The Emerging Standard for Corporate Compliance, IT Governance Ltd., 2008, ISBN 978-1-905356-66-9

[5] James S. Plank, Scott Simmerman, Catherine D. Schuman, Jerasure: A library in C/C++ Facilitating Erasure Coding for Storage Applications-Version 1.2. Technical Report CS-08-627, University of Tennessee, August 2008, www.cs.utk.edu/~plank/plank/papers/CS-08-627.pdf

[6] Hakim Weatherspoon, John D. Kubiatowicz, Erasure Coding vs. Replication: A Quantitative Comparison, University of California, Berkeley, March 2002., www.cs.rice.edu/Conferences/IPTPS02/170.pdf

[7] Maxim Schnjakin, Rehab Alnemr, Christoph Meinel, A security and high-availability layer for Cloud-Storage, in: Web Information Systems Engineering – WISE 2010 Workshops, volume 6724 of Lecture Notes in Computer Science, S. 449, Springer, 2011, ISBN 978-3-642-17615-9

[8] Maxim Schnjakin, Christoph Meinel, Implementation of Cloud-RAID: A Secure and Reliable Storage Above the Clouds, in: Proceedings of 8th International Conference on Grid and Pervasive Computing – GPC 2013, Springer, 2013, ISBN 978-3-642-38026-6

[9] Maxim Schnjakin, Dimitri Korsch, Martin Schoenberg, Christoph Meinel, Implementation of a Secure and Reliable Storage Above the Untrusted Clouds, in: Proceedings of 8th International Conference on Computer Science and Education – ICCSE 2013, Springer

[10] Maxim Schnjakin, Christoph Meinel, Plattform zur Bereitstellung sicherer und hochverfügbarer Speicherressourcen in der Cloud, in: Sicher in die digitale Welt von morgen, Tagungsband des 12. Deutschen IT-Sicherheitskongresses des BSI, SecuMedia, 2011, ISBN 978-922746-96-6