Hans Pongratz

# Cloud Computing: Universitäre Einsatzszenarien & Erfahrungen

Echte Chance oder purer Hype?

**Der Trend des Cloud Computing wurde die letzten Jahre viel diskutiert und erfreut sich zunehmender Beliebtheit. Die Technische Universität München (TUM) setzt bereits seit vielen Jahren im Rahmen der IT-Strategie „Digitale Hochschule“ verschiedene Cloud-Computing-Dienste ein. Der Begriff steht für die bedarfsgerechte Nutzung von IT-Ressourcen, welche entweder über ein Intranet oder über das Internet angeboten werden. Die Abrechnung erfolgt meist verbrauchsorientiert. Durch die Verlagerung des Betriebs der genutzten Dienste auf externe Stellen sollen eine bessere Skalierbarkeit, eine höhere Flexibilität und in der Gesamtschau auch niedrigere Kosten erreicht werden.**

Der sogenannte Cloud-Stack (s. Abb. 1) stellt als pyramidenförmiges Dreischichtenmodell die Architektur und Vielfalt der denkbaren Einsatzszenarien für Cloud Computing dar. Die einzelnen Schichten können aufeinander als Cloud-Dienste aufbauen, müssen es aber nicht. Die Basis der Pyramide bildet die IT-Infrastruktur, welche als Infrastructure-as-a-Service (IaaS) bezeichnet wird. Typische Anwendungsbeispiele sind die Nutzung von virtuellen Servern, Archivierungs- und Backupsystemen oder auch Netzwerkdiensten, welche über das Internet zur Verfügung gestellt und zum Beispiel je nach verbrauchter Rechenzeit oder Speicherplatznutzung bezahlt werden. Die Mitte der Pyramide bildet die sogenannte Plattformschicht für Anwendungsentwicklung, Platform-as-a-Service (PaaS). Diese ermöglicht es, eigene Anwendungen in einer standardisierten, bedarfsorientierten Umgebung zu betreiben. Der PaaS-Anbieter stellt notwendige Updates, Sicherungen und ausreichend Rechen-, Netzwerk- und Speicherkapazität sicher. Die Spitze der Pyramide ist die Anwendungsschicht, Software-as-a-Service (SaaS) genannt. Hier wird eine meist hochverfügbare, performante Anwendung eines Cloud-Anbieters genutzt, der Nutzer muss sich weder um den Betrieb der Infrastruktur noch um die Plattform kümmern.

**Stichwörter**
Cloud Computing
Cloud-Dienste
Datenschutz
IT-Trend

Bei der Organisationsform von Clouds wird hauptsächlich zwischen öffentlichen (Public) und nicht-öffentlichen (Private) Clouds unterschieden. Public Clouds bieten Dienste, welche quasi von jedem weltweit genutzt werden können und bringen somit einige Herausforderungen im Bereich der Datensicherheit und des Datenschutzes mit sich. Private Clouds stehen nur organisationsintern zur Verfügung und sind gegenüber Zugriffen von außerhalb der Organisation abge-

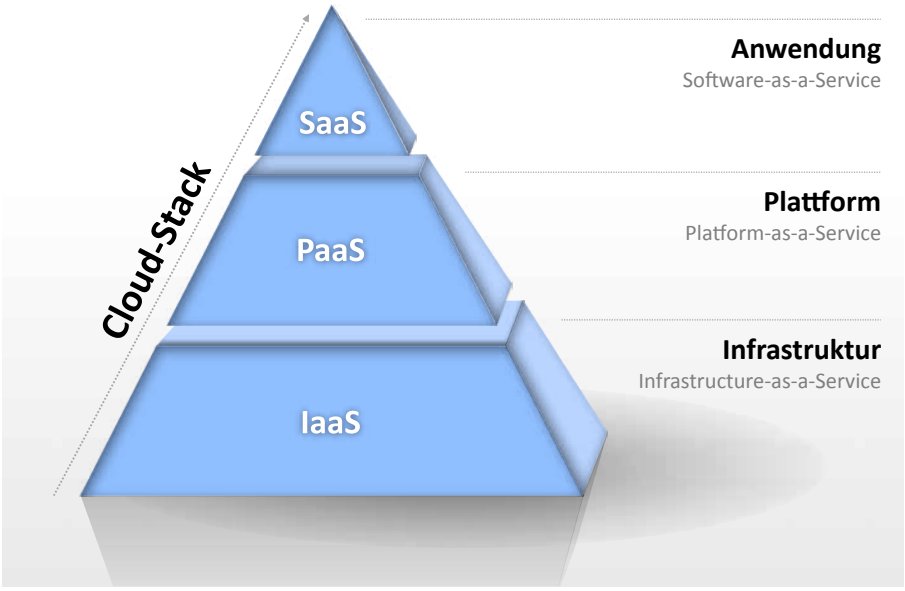


*Abb. 1: Cloud-Stack*

schottet. Eine Mischform von Private und Public Cloud wird Hybrid Cloud genannt. Hier werden bestimmte Dienste innerhalb der eignen Organisation betrieben und andere von Public Cloud-Anbietern über das Internet.

**Vorarbeiten für die Nutzung von Cloud-Diensten**

Vor der Nutzung von Cloud-Diensten sollte eine Standardisierung und Vereinheitlichung der Anforderungen erfolgen. Dies gilt unabhängig der gewünschten Cloud-Architektur und Organisationsform. Es muss klar sein, welche Geschäftsprozesse vom Cloud-Service in welchem Umfang, mit welcher Verfügbarkeit und zu welchen Kosten erbracht werden sollen. Im Rahmen eines Service-Level-Agreement (SLA) werden die Anforderungen mit dem jeweiligen Anbieter transparent fixiert und Metriken zur Überwachung der Diensterbringung vereinbart. Häufig verwendete Metriken sind: die Verfügbarkeit des Service, die Zeit zur Wiederherstellung des Betriebs nach einem Ausfall, die durchschnittliche Zeit vom Ausfall bis zur Wiederinbetriebnahme, die Zeit zwischen zwei Ausfällen und deren Durchschnittswert. Im Rahmen des SLA werden auch weitere Leistungsbeschreibungen, wie zum Beispiel die Betriebszeiten des Dienstes (24x7) und die Servicezeiten (Mo - Fr, 8 - 18 Uhr) festgelegt. Natürlich müssen SLAs regelmäßig, nicht nur bezüglich der Erfüllung, sondern auch zur Passgenauigkeit auf die sich ändernden Bedürfnisse geprüft und bei Bedarf überarbeitet werden. Ebenso sollte das Identity Management geplant werden – wie soll der Provisierungs- und der spätere Deprovisionierungsworkflow für Accounts ablaufen? Im Idealfall kann auf einen zentralen Verzeichnisdienst zurückgegriffen und die Authentifikation beim Cloud-Dienst über eine Single-Sign-On-Lösung (SSO), zum Beispiel per Shibboleth, durchgeführt werden.

**Datenschutz**

Für öffentliche Landeseinrichtungen, wie zum Beispiel Hochschulen, gilt das jeweilige Landesdatenschutzgesetz, welches sich vom Bundesdatenschutzgesetz und der EU-Datenschutzrichtlinie 95/46/EG mehr oder weniger ableitet. In diesen Landesgesetzen sind Regeln zum Umgang mit personenbezogenen Daten und zur Auftragsdatenverarbeitung definiert und somit die Pflichten der jeweiligen Einrichtung dargelegt. Auf den Punkt gebracht muss bei einer Auftragsdatenverarbeitung

Shibboleth ist ein Verfahren zur verteilten Authentifizierung und Autorisierung für Webanwendungen und Webservices. Das Konzept von Shibboleth sieht vor, dass der Benutzer sich nur einmal bei seiner Heimateinrichtung authentisieren muss, um ortsunabhängig auf Dienste oder lizenzierte Inhalte verschiedener Anbieter zugreifen zu können.

*Quelle: Wikipedia*

Hans Pongratz ist Geschäftsführender Vizepräsident und Chief Information Officer (CIO) der Technischen Universität München.

die Auftrag gebende Stelle sicherstellen, dass keine personenbezogenen Daten an unbefugte Dritte gelangen. Die personenbezogenen Daten dürfen vom Auftragnehmer auch nur so weit verarbeitet und gespeichert werden, wie es der Auftraggeber anordnet. Hier besteht ein klares Weisungsverhältnis. Der Auftragnehmer darf die Daten zu keinem anderen Zweck selbst weiterverwenden. Der Auftraggeber muss sich in regelmäßigen Abständen vergewissern, dass der Auftragnehmer korrekt handelt und das Verfahren anhand einer Verfahrensbeschreibung vom Datenschutzbeauftragten der eigenen Organisation freigeben lassen. Bei der Funktionsübertragung findet rechtlich gesehen eine Datenübermittlung statt und der Auftragnehmer ist für die Einhaltung des Datenschutzes und der Datensicherheit selbst verantwortlich. Außerdem muss eine wirksame Einwilligung aller Betroffenen bezüglich der Übermittelung der Daten vorliegen oder eine „Übermittlung an Dritte“ nach Landesdatenschutzgesetz erlaubt sein. Erfolgt die Datenverarbeitung außerhalb der EU und des Europäischen Wirtschaftsraums (EWR) ergeben sich daraus noch besondere Anforderungen. Einige internationale Cloud-Anbieter garantieren daher inzwischen die Verarbeitung und Speicherung der personenbezogenen Daten innerhalb des EWR. Die Informationsseite des Bayerischen Datenschutzbeauftragten (http://www.datenschutz-bayern.de/technik/orient/oh_auftragsdatenverarbeitung.html) beinhaltet weitere Informationen und eine Orientierungshilfe zur Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung. Eine frühzeitige Konsultation des zuständigen Datenschutzbeauftragten ist auf alle Fälle sehr empfehlenswert. Sofern personenbezogene Daten von Beschäftigten erhoben, verarbeitet oder genutzt werden, kann eine Dienstvereinbarung mit dem zuständigen Personalrat notwendig sein.

**keywords**
cloud computing
cloud services
data protection
it trend

### Sicherheit & Herausforderungen

Aufgrund fehlender Standards und Sicherheitsbestimmungen gestaltet sich die Risikoanalyse von Public-Cloud-Anbietern und deren Diensten schwierig. Die Bedrohungsszenarien reichen vom klassischen Datenleck über Denial-of-Sevice-Attacken bis zur Datenmanipulation. Auch die Gefahr einer Insolvenz des Anbieters oder die Beschlagnahmung von Hardware sollten bei den Überlegungen berücksichtigt werden. Insofern muss im Vorfeld bereits sehr kritisch abgewogen werden, welche Geschäftsdaten und -prozesse auf Cloud-Dienste verlagert, welche Schutzmaßnahmen notwendig sind und wie diese vertraglich festgelegt und kontinuierlich überwacht werden können. Teil der notwendigen Schutzmaßnahmen können externe Backups, die redundante Datenhaltung und die Verschlüsselung der Daten sein. Zu den weiteren Herausforderungen gehören die Abhängigkeit von der Stabilität und der zur Verfügung stehenden Bandbreite der Internetverbindung. Auch die Erreichbarkeit des Dienstanbieters und der sogenannt Lock-in-Effekt, also die Abhängigkeit vom jeweiligen Cloud-Anbieter, sollten im Vorfeld bedacht und je nach Bedarf Alternativen beziehungsweise Ausstiegsstrategien geplant werden.

### Einsatzszenarien & Erfahrungen

Die denkbaren Einsatzszenarien von Cloud-Diensten für Hochschulen sind sehr vielfältig und reichen von der Nutzung von Rechenzeit bis zum Einsatz eines Sozialen Netzwerkes. Tabelle 1 gibt einen beispielhaften Überblick.

Das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften ist das gemeinsame Rechenzentrum der beiden Münchner Universitäten, der Ludwig-Maximilians-Universität München (LMU) und TUM, sowie der Bayerischen Akademie der Wissenschaften. In den letzten Jahren wurde eine Vielzahl an hochverfügbaren, mandantenfähigen Private-Cloud-Diensten im LRZ aufgebaut, von denen im Folgenden eine Auswahl vorgestellt wird. Grundlage für die Arbeiten war das Großprojekt IntegraTUM, welches die Schaffung einer benutzerfreundlichen und nahtlosen Infrastruktur für Information und Kommunikation (IuK) an der TUM zum Ziel hatte und

**summary**

Cloud Computing for higher education institutions: hype or sustainable opportunity? Service & deployment models, challenges and experiences.

durch Mittel der Deutsche Forschungsgemeinschaft (DFG) und der InnovaTUM-Initiative gefördert wurde. Der Umfang der Dienste ist im Rahmen eines jährlich aktualisierten Dienstleistungskatalogs klar geregelt.

| Architektur | Beispielhafte Einsatzszenarien für Hochschulen |
|---|---|
| Infrastruktur (IaaS) | Virtuelle Server<br>Speicher<br>(wissenschaftliche) Rechenzeit |
| Plattform (PaaS) | Entwicklungsumgebung<br>Laufzeitumgebung |
| Anwendung (SaaS) | Office Anwendungen<br>Social Media (Foren, Wikis, Blogs, Podcasts, Soziale Netzwerke, …)<br>Plagiatspräventionssoftware<br>Veranstaltungsmanagement<br>Projektmanagement |

*Tab. 1: Übersicht beispielhafter Einsatzszenarien für Hochschulen*

Als IaaS-Architektur wird ein zentraler Verzeichnisdienst als Grundlage des Identity Managements der TUM auf virtuellen Servern des LRZ betrieben und von Mitarbeitern der TUM administriert. Ebenso auf virtuellen Servern ist das zentrale E-Learning-System der TUM, Moodle, installiert. Die virtualisierten, hochverfügbaren Serverinstanzen werden vom LRZ auf eigener Server-Hardware mit unterbrechungsfreier Stromversorgung und 24-Stunden-Überwachung betrieben. Das LRZ kümmert sich um die Installation und Pflege des Betriebssystems und der Hardware. Die TUM ist für die Installation und Administration der Anwendung(en) verantwortlich.

Ein weiterer IaaS-Dienst ist die Private Storage Cloud: Alle Studierende und Beschäftigte der TUM haben ein persönliches, hochverfügbares, Snapshot-gesichertes und zugriffsgeschütztes Speicherplatzkontingent von 20GB und maximal 80.000 Dateien. Per VPN-Verbindung kann es problemlos angebunden werden und ist auch per Weboberfläche erreichbar. Ein temporäres Laufwerk dient dem Austausch von Daten. Dort abgelegte Dateien werden nach zwei Tagen automatisch gelöscht. Projektverzeichnisse können für Arbeitsgruppen über den zuständigen Information Officer der jeweiligen Fakultät beziehungsweise zentralen Einrichtung eingerichtet werden.

Als SaaS-Lösungen stehen ein zentraler Groupware Dienst (MS Exchange 2010) und Typo3-Instanzen als TUM-Typo3-Site mit einheitlichem Corporate Design und zentralem Schulungs- und Supportangebot zur Verfügung und erfreuen sich starker Nachfrage.

Zusätzlich hat sich die TUM für die Nutzung einiger Public-Cloud-Dienste auf freiwilliger Basis entschieden. Dazu gehören eine Wiki-Plattform, eine Veranstaltungsmanagement-Lösung, ein Tool zur Plagiatsprüfung von wissenschaftlichen Arbeiten und eine Vorlesungsaufzeichnungsplattform. Die beiden zuletzt genannten Lösungen werden zurzeit evaluiert. Die Wiki-Plattform konnte direkt an das zentrale Identity-Management per Shibboleth angebunden werden und fügt sich somit nahtlos für die Nutzer in die Gesamtinfrastruktur ein.

## Fazit

Cloud Computing bringt viele Vorteile, aber auch einige, vor der Nutzung zu thematisierende Herausforderungen mit sich. Der Reifegrad vieler Cloud-Lösungen ist inzwischen sehr hoch und die meist modularen Dienste lassen sich auch schrittweise um neue Funktionalitäten erweitern und in eine bestehende Infrastruktur schnell und einfach integrieren. Auch die Abrechnung nach tatsächlicher Nutzung, die meist kurzen Mindestvertragslaufzeiten und die Verlagerung der Verantwortung zur Wartung und Fortentwicklung des Dienstes auf den Anbieter sind sehr positiv zu sehen. Noch in der Diskussion ist die Umwandlung von öffentlichen Fördermitteln für die Beschaffung von Servern für das wissenschaftliche Rechnen. Diese Investitionsgelder können noch nicht für den Kauf von Rechenzeit von einem Cloud-Anbieter eingesetzt werden. Aus Sicht der TUM hat sich in den letzten Jahren vor allem der Einsatz von Private-Cloud-Lösungen, unter anderem zur Rezentralisierung von IT-Basisdiensten wie E-Mail- oder Webserver, sehr bewährt und wird im Rahmen der IT-Strategie in den nächsten Jahren weiter ausgebaut werden.

**Kontakt:**

**Dipl.-Inf. Hans Pongratz**
**Geschäftsführender Vizepräsident**
**und Chief Information Officer (CIO)**
**Technische Universität München**
**Arcisstr. 21**
**80333 München**
**Tel.: +49 (0) 89 289 28240**
**E-Mail: pongratz@tum.de**
**www.tum.de**