Entwicklung und Implementierung einer Ontologie für das IT-Sicherheitsmanagement im Cloud Computing

Matthias Gräuler, Benedikt Martens, Frank Teuteberg

Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik
Universität Osnabrück
Katharinenstr. 1
49069 Osnabrück
{matthias.graeuler, benedikt.martens, frank.teuteberg}@uni-osnabrueck.de

Abstract: Cloud Computing hat sich in den letzten Jahren zu einem Hype-Thema in Unternehmen entwickelt. Besondere Aufmerksamkeit wird in diesem Zusammenhang der IT-Sicherheit im Cloud Computing geschenkt. Vor allem deutsche Unternehmen stehen diesem Thema äußerst kritisch gegenüber und führen häufig umfangreiche Evaluationsstudien über potenziell zu implementierende Cloud-Computing-Dienste durch. Kritisch werden hier vor allem die vom Anbieter implementierten Sicherheitsmaßnahmen und Kontrollen analysiert, da sie häufig nicht im Einflussbereich der Anwender liegen. Im Rahmen dieses Beitrages wird eine Ontologie für das IT-Sicherheitsmanagement im Cloud Computing sowie eine Weboberfläche für die Formulierung von Abfragen an die Ontologie vorgestellt. Ziel der entwickelten IT-Artefakte ist die Sammlung und Präsentation von Wissen über von ausgewählten Cloud-Computing-Anbietern implementierten Sicherheitsmaßnahmen, der Vergleich dieser Maßnahmen sowie das Aufzeigen von möglichen Risiken. Damit wird das übergeordnete Ziel verfolgt, Entscheidungsträgern ein Werkzeug zur Verfügung zu stellen, das es ihnen erleichtert, datenschutzrelevante Informationen in ihre Entscheidungen mit einzubeziehen.

1 Einleitung und Motivation

Durch das Aufkommen des Cloud Computing in den letzten Jahren haben sowohl Unternehmen als auch Privatanwender viele Vorteile aus dem neuen IT-Outsourcing-Modell ziehen können: Schnell skalierbare Infrastrukturen, hohe Verfügbarkeit und ein Preismodell, bei dem nur gezahlt werden muss, was tatsächlich verbraucht wurde sind nur einige der zahlreichen Vorteile ([Mil09a], [Mil09b]). Doch auch neue Risiken entstehen durch diese Form des IT-Outsourcings. Durch das Fehlverhalten einzelner Kunden können auch andere beeinträchtigt werden, die neue Infrastruktur schafft neue Angriffsvektoren ([Ris09]) und sensible Daten sollten nicht ohne weiteres an die Anbieter weitergegeben werden ([MT09]). Auch Anbieter von Cloud-Computing-Diensten beschäftigen sich mit diesen Problemen.

In diesem Beitrag wird eine Ontologie vorgestellt, die sicherheitsrelevantes Wissen zu Cloud-Computing-Diensten und -Anbietern enthält und gleichzeitig aufzeigt, wie Anbieter weitere Risiken vermeiden können. Um einer möglichst breiten Anwendergruppe aus Wissenschaft und Praxis den Zugang zu der Ontologie zu ermöglichen, wurde eine

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Weboberfläche in PHP und JavaScript implementiert, welche es den Benutzern ermöglicht vordefinierte und freie Abfragen an die Ontologie zu stellen, um vorhandenes Wissen zu extrahieren.

Im Folgenden wird zunächst der Begriff des Cloud Computing definiert und die technische Basis, eine Community-Plattform, die Informationen zu bestehenden Cloud-Computing-Anbietern und -Diensten enthält, vorgestellt. Weiterhin werden verwandte Forschungsarbeiten diskutiert und das methodische Vorgehen bei der Erstellung der IT-Artefakte erläutert. In den Abschnitten 6 und 7 werden die jeweiligen IT-Artefakte und ihre Entwicklung erläutert. Abschließend werden die erbrachten Leistungen im Abschnitt 8 evaluiert und in Abschnitt 9 ein Ausblick auf zukünftige Forschungsarbeiten gegeben.

2 Cloud Computing

Cloud Computing wird häufig mit dem schon länger praktizierten Grid Computing verglichen ([Wei09]). Während die Nutzung von Grid Computing abnimmt, da nur sehr wenige Geschäftsmodelle aus der Technologie hervorgegangen sind und ihre Förderung, die meist aus staatlichen Quellen stammt, ausbleibt ([Gen08]), steigt die Popularität des Cloud Computing ([PwC10]). Das National Institute of Standards and Technology (NIST) schlägt folgende Definition für das Cloud Computing vor ([MG09]):

> *„Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential* ***characteristics,*** *three* ***service models****, and four* ***deployment models****."*

Als Charakteristika des Cloud Computing werden die automatisierte Erweiterung von Ressourcen, die Notwendigkeit von Breitband-Internetanbindungen, die gemeinsame Nutzung eines Ressourcenpools durch die Benutzer, eine schnelle Skalierbarkeit und ein automatisiertes Monitoring zur Gewährleistung der Transparenz genannt.

Es wird weiterhin zwischen drei Dienstmodellen unterschieden, die aufgrund ihrer Anfangsbuchstaben auch mit dem Akronym „SPI" bezeichnet werden ([OBM10]):

- Software as a Service (SaaS), das die Nutzung von Anwendungen über Thin Clients, wie z. B. mittels eines Browsers, ermöglicht;
- Platform as a Service (PaaS), das häufig Entwicklungs- und Laufzeitumgebungen für diverse Programmiersprachen zur Verfügung stellt und
- Infrastructure as a Service (IaaS), durch das fundamentale Ressourcen, wie z. B. Rechenleistung oder Speicherplatz, über das Internet verfügbar gemacht werden

ISBN 978-3-88579-286-4

Die Art der Bereitstellung unterscheidet sich in ([MG09]):

- Private Clouds, die nur für eine einzelne Organisation Leistungen erbringen;
- Community Clouds, in denen die Ressourcen der Cloud von mehreren Organisationen mit bestimmten Gemeinsamkeiten geteilt werden;
- Public Clouds, wobei die Dienste für die breite Öffentlichkeit verfügbar sind und außerdem
- Hybrid Clouds, die einen Zusammenschluss von mindestens zwei Clouds unterschiedlicher Bereitstellungsarten darstellen.

Besonders bei Public Clouds sollte bei der Auswahl eines Anbieters großes Augenmerk auf die verwendeten Sicherheitsmaßnahmen gelegt werden ([Wei09]). Public Clouds werden von mehreren Mandanten gleichzeitig genutzt, wobei die rechtliche Verantwortung für eine ordnungsgemäße, sichere und gesetzeskonforme Datenverarbeitung beim Auftraggeber selbst verbleibt ([Bit06], S. 18).

Die Abrechnung der Leistungen erfolgt nutzungsabhängig, d. h. dass i. d. R. keine Grundgebühren anfallen und nur in Rechnung gestellt wird, was tatsächlich genutzt wurde. Als Metriken hierfür werden bspw. je nach Dienstmodell die Anzahl der Benutzer, die Menge des Datentransfers, verbrauchte Rechenzeit o. Ä. herangezogen. Cloud Computing bietet sich vor allem in Szenarien an, in denen starke Schwankungen oder Anstiege der benötigten Rechnerleistungen zu erwarten sind ([Arm09]). Dies können z. B. eine saisonal-abhängige Nachfrage in einem Onlineshop oder ein schnelles Wachstum bei einem Start-Up-Unternehmen sein. Als Treiber für das Cloud Computing gelten die Nutzung von großen Rechenzentren, die eine effiziente Ausnutzung der sich dadurch ergebenden Skaleneffekte möglich machen ([Arm09]), der inzwischen hohe Verbreitungsgrad von Breitbandinternetverbindungen und Fortschritte der Virtualisierungstechniken ([YBS08]). Das vermehrte Aufkommen von Green IT ([Ber09]) und ein gestiegener Kostendruck durch die Weltwirtschaftskrise im Jahr 2009 trugen ebenfalls zu dieser Entwicklung bei. Neben Unternehmen und Privatpersonen nutzen auch öffentliche Verwaltungen Dienste aus der Cloud; bspw. setzt die Stadt Los Angeles bereits seit 2009 den SaaS-Dienst „Google Mail“ für 30.000 Angestellte ein. In Deutschland hingegen lässt eine derartige Entwicklung noch auf sich warten ([Sin10]).

3 Community-Plattform CloudServiceMarket.info

Aufgrund der Vielschichtigkeit und der hohen Anzahl der öffentlich angebotenen Cloud-Computing-Dienste ist es schwierig einen Überblick über den Cloud-Computing-Markt zu gewinnen ([MTG11]). Um Informationen über die verschiedenen Angebote zu erhalten, ist mitunter eine aufwändige Recherche notwendig. Diese Recherche enthält, selbst wenn sie gründlich durchgeführt wird, unter anderem aufgrund der inkonsistenten Namensgebungen der Dienstarten, nicht alle möglichen Dienste. Außerdem mangelt es an einer neutralen und ausführlichen Evaluation der Anbieter und Dienste, da diese vor

Einführung der in [MTG11] vorgestellten Plattform nur anhand von den von den Anbietern selbst zur Verfügung gestellten Informationen vorgenommen werden konnte.

Die von den Autoren dieses Beitrags entwickelte Community-Plattform CloudServiceMarket.info (www.cloudservicemarket.info) beinhaltet derzeit 207 Dienste von 179 Anbietern (Juli 2011), die Anhand einiger Leistungsparameter, wie bspw. Dienstkategorien, Zertifizierungen, Compliance-Regelungen oder Standorte der Rechenzentren erfasst sind. Mithilfe zweier Suchmasken, jeweils eine für die Anbieter und Dienste, kann das erfasste Angebot durchsucht werden. Für jeden Anbieter und jeden Dienst steht eine eigene Seite zur Verfügung auf der Informationen eingesehen werden können. Darüber hinaus kann jeder registrierte Benutzer Bewertungen für sowohl Anbieter als auch Dienste verfassen, mit denen er bereits Erfahrungen gesammelt hat. Diese Bewertungen können entweder in einfacher Form mit einem Kommentar und einer Bewertung auf einer Skala von eins („keine Empfehlung“) bis 5 („Empfehlung“) oder ausführlich mit Kommentaren und Bewertungen zu sieben Kategorien, wie z. B. Support/Kommunikation mit Anbieter, Schnittstellen oder Kostenübersicht/-kontrolle, vorgenommen werden. Da diese Bewertungen subjektiven Eindrücken unterliegen und nur mit hohem Aufwand auf ihren Wahrheitsgehalt überprüft werden können, wird es Benutzern in einer zukünftigen Version von CloudServiceMarket.info möglich sein die Bewertungen anderer Benutzer wiederum zu kommentieren und so Feedback zu der erwähnten Kritik zu geben. Des Weiteren können Benutzer neue Dienste und Anbieter über entsprechende Masken einsenden. Darüber hinaus werden Informationen zu Forschern, Forschungsprojekten und Studien zum Thema Cloud Computing gesammelt.

4 Verwandte Forschungsarbeiten

Ausgangspunkt der Ontologieentwicklung ist eine Literatur- und Onlinerecherche, um den aktuellen Stand der Forschung aufzuarbeiten und Beiträge, die ebenfalls zum Ziel haben Semantic Web Technologien mit dem Cloud Computing zu verknüpfen, zu identifizieren und zu analysieren. Durch die Anwendung der Vorgehensmodelle in [WW02] sowie [Bro09] für einen systematischen Literatur-Review wurden vorhandene Arbeiten möglichst vollständig identifiziert. Hierzu wurde mit Hilfe von Suchmaschinen (z. B. Google Scholar), akademischen Journaldatenbanken (z. B. EBSCO, AISeL, Science Direct), den Suchfunktionen renommierter wissenschaftlicher Verlage (u. a. Springer, ACM) und wissenschaftlichen Konferenzen (z. B. ICIS, ECIS, AMCIS, WI) nach Wortkombinationen wie bspw. „IT Security Ontology“, „Cloud Computing Ontology“ und weiteren Variationen gesucht.

De Oliveira et al. ([OBM10]) stellen eine umfassende Taxonomie des Cloud Computing vor und schlagen weitere Untertaxonomien für die acht Bereiche Architektur, Geschäftsmodell, technologische Infrastruktur, Bereitstellungsart, geltende Standards, preisliche Ausgestaltung, Benutzer-/Aufgabenorientierung und Zugangsart vor. Ausgangspunkt der Taxonomieentwicklung ist die bisher nicht einheitliche Definition des Cloud Computing. Das Ziel ist die Klassifikation von Konzepten innerhalb dieser Domäne, um eine Grundlage für z. B. Ontologien zu entwickeln.

In [FE09] wird von Fenz und Ekelhart eine ausführliche Ontologie zur Formalisierung von Wissen bzgl. der Informationssicherheit vorgestellt, die sich an den Vorgaben in [GR95] orientiert. Das beinhaltete Wissen ist jedoch nicht auf das Cloud Computing zugeschnitten, so fehlen z. B. Verweise auf korrespondierende SLAs, und enthält Sachverhalte, die für diese Anwendungsdomäne irrelevant sind, wie z. B. die Sicherheit einzelner Räumlichkeiten.

Takahashi et al. schlagen in [TKF10] eine Ontologie vor, die im operativen Geschäft von Firmen zur Verbesserung des Sicherheitsmanagements angewandt werden soll. Dies steht im Kontrast zu der im Folgenden vorgestellten Ontologie, die zum Ziel hat Defizite und Stärken hinsichtlich des Sicherheitsmanagements von Cloud-Computing-Diensten und -Anbietern aufzuzeigen.

Schließlich stellen Han und Sim in [HS10] „Cloudle“, ein sog. Cloud Service Discovery System vor. Das System stellt eine Datenbasis zur Verfügung, die von Benutzern durchsucht werden kann und mit Hilfe von Ähnlichkeitsmaßen auf der Basis der Dienstparameter mehrere Dienste empfiehlt ([KS10]). Hierfür werden die in einer Ontologie hinterlegten relevanten Konzepte miteinander verknüpft und für jeden durchsuchten Dienst ein aggregierter Nutzwert errechnet. Je näher dieser Nutzwert an 1,0 liegt, umso eher entspricht er den gesuchten Kriterien.

Die Analyse der verwandten Forschung hat aufgezeigt, dass bisher nur wenige Arbeiten auf eine Verbindung der Ontologieentwicklung und dem Cloud Computing abzielen. Die in [HS10] vorgestellten Ergebnisse wenden zwar beide Konzepte an, jedoch ist grundsätzlich zu erkennen, dass der Fokus auf die Informations- und Datensicherheit nur begrenzt ist. Vor allem vor dem Hintergrund der praktischen Relevanz dieses Themas besteht auf diesem Gebiet noch hoher Forschungsbedarf. Die in den Arbeiten aufgeführten Ergebnisse werden als Basis für die in diesem Beitrag zu entwickelnden IT-Artefakte verwendet, bauen darauf auf und erweitern diese.

5 Methodisches Vorgehen

Die Auswahl eines geeigneten Ontologieeditors wird größtenteils von der Auswahl der Ontologiesprache diktiert. Einer Empfehlung des W3Cs ([W3C09]) folgend, wurde OWL 2 ausgewählt. Somit kommen nur Editoren in Frage, die diese Ontologiesprache unterstützen. In [KBM08] wird eine Vielzahl von Ontologieeditoren bewertet, allerdings unterstützen nicht alle von ihnen OWL 2. Weitere Kriterien sind fortlaufende Weiterentwicklungen des jeweiligen Ontologieeditors um zu gewährleisten, dass die Ontologie auch in Zukunft noch gepflegt werden kann. Nach Anwendung dieser Kriterien fiel die Wahl auf den Ontologieeditor „Protégé“ ([Gen03]).

Um die in der Ontologie erfassten Daten benutzen zu können, ist eine spezielle Abfragesprache notwendig. OWL-Ontologien, die im Extensible Markup Language (XML)/Resource Description Framework (RDF) Format gespeichert werden, können mittels der vom W3C standardisierten Sprache SPARQL abgefragt werden.

Bei der Ontologieerstellung wurde auf die Forschungsmethode des Prototypings zurückgegriffen, wobei eine schnell verfügbare, lauffähige Vorabversion eines Anwendungssystems entwickelt und evaluiert wird ([WH06]). Diese Prototypen werden in üblicherweise mehreren Iterationen entweder evolutionär zu nachfolgenden Prototypen weiterentwickelt, inkrementell um weitere Funktionen ergänzt oder verworfen ([Dav92]). Wie im Weiteren erläutert wird, wurde eine Kombination aus dem evolutionären, als auch dem Throw-Away-Ansatz verfolgt. Während der Arbeit an der Ontologie wurden zusätzlich Experteninterviews zur konzeptionellen Evaluation durchgeführt. Unter einem Experteninterview wird ein leitfadengestütztes Interview einer Person verstanden, die sich durch Expertenwissen im Forschungsgebiet hervortut ([LT09]). Nach der Fertigstellung des ersten Prototypen der Ontologie begannen die Arbeiten an der Implementierung, die ebenfalls evolutionär in der Skriptsprache PHP erfolgten.

6 Konzeption der Ontologie

Bevor die einzelnen Beziehungen innerhalb der Ontologie erläutert werden, wird nachfolgend ein Überblick der gesamten Ontologie vorgestellt. Eine geeignete Form der Repräsentation einer Ontologie ist ein UML-Klassendiagramm ([Cra01]), die auch bei der nachfolgenden Abbildung 1 gewählt wurde.

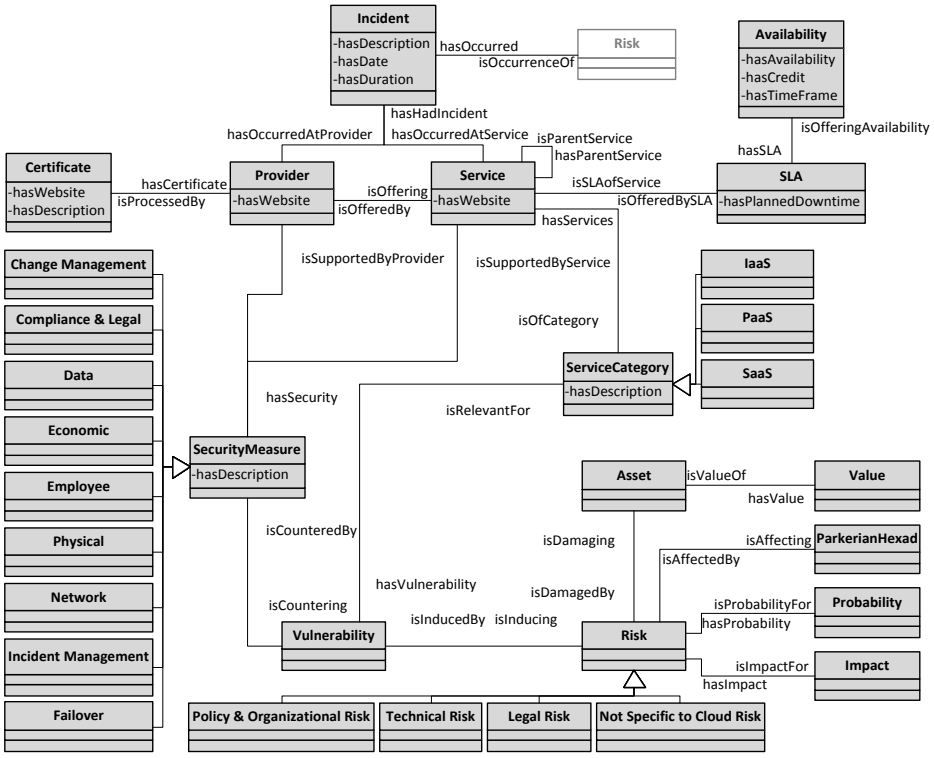

Abbildung 1: Klassendiagramm der Ontologie

In der Ontologie werden die Dienste und Anbieter nur sehr rudimentär beschrieben, so beschränken sich dessen Beschreibungen auf ihren Namen und eine URL zu einer offiziellen Informationsseite. Der Informationsgehalt wurde bewusst gering gehalten, da andere Informationen bereits in der CloudServiceMarket.info-Datenbank enthalten sind und die Ontologie ergänzt werden soll. Für die Darstellung der Funktionen und Auswertungsmöglichkeiten werden als Datenbasis sieben Dienste der drei Anbieter Microsoft, Google und Amazon Web Services (AWS) untersucht. Der Hintergrund ist vor allem der hohe Informationsgehalt, der über die Internetseiten der Anbieter verfügbar ist und somit keine weiteren Recherchen notwendig sind.

Die Klasse „Service“ besitzt eine Parent-Child Relation mit sich selbst. Dies geschieht um bspw. zu erfassen, dass der Dienst „Dropbox“ den „Simple Storage Service“ („S3“) von AWS zur Datenhaltung nutzt, und ihm somit die von AWS realisierten Sicherheitsmaßnahmen „vererbt“ werden. Die Anbieter erwerben häufig bestimmte Zertifizierungen ([MTG11]), die den potenziellen Nutzern signalisieren, dass sie bestimmte Standards wie bspw. Compliance, Auditierung, aber auch Sicherheit einhalten. Zu den am häufigsten anzutreffenden Zertifizierungen zählen die allgemeingültigen SAS 70, ISO 27001 und Safe Harbor sowie anwendungsspezifische wie FISMA, PCI DSS und HIPAA ([MTG11]). Die Erfassung der Einhaltung dieses Kriteriums geschieht über die Beziehung zwischen den Klassen „Provider“ und „Certificate“. Ein weiteres wichtiges Kriterium zur Auswahl eines Dienstes ist deren Verfügbarkeit. Durch die Service Level Agreements (SLA) werden z. B. Verfügbarkeiten und Gutschriften bei Unterschreitung von zugesicherten Service Levels geregelt. Diese Eigenschaft wird durch die Beziehung der Klassen „Service“, „SLA“ und „Availability“ dargestellt. In der Klasse „SLA“ wird weiterhin erfasst inwiefern mögliche Wartungszeiten die Bereitstellung und Verfügbarkeit beeinflussen und somit nicht auf die Verfügbarkeit angerechnet werden.

Um IT-Risiken in einem allgemeinen Kontext in der Ontologie zu berücksichtigen, werden die drei Konstrukte Risks (Risiken), Vulnerabilities (Schwächen) und Assets (Werte) verwendet ([Eni09]). Abbildung 2 illustriert deren Ursachen-Wirkungszusammenhang: Durch ausgenutzte Schwächen können Risiken entstehen, die wiederum das Potenzial besitzen die Unternehmenswerte, wie z. B. das Vertrauen der Kunden, zu beschädigen. Im Umkehrschluss bedeutet dies, dass um die Werte zu schützen, die Risiken, die zu deren Beschädigung führen können, reduziert werden müssen, indem die Schwächen beseitigt werden. Würde bspw. bei einem Anbieter die Schwäche „Ungenügende physische Sicherheitsmaßnahmen“ vorliegen, würde dies das Risiko „Diebstahl von Computerausstattung“ begünstigen, welches wiederum die Werte „Personenbezogene Daten“, „Daten des Personalwesens“ und „Physische Hardware“ in negativer Weise beeinflusst ([Eni09, S. 52]).

Abbildung 2: Zusammenhänge von Schwächen, Risiken und Werten

In [Eni09] werden 53 Schwächen, 23 Werte und 35 Risiken des Cloud Computing identifiziert und untereinander verknüpft. Die aufgeführten Risiken sind weiterhin in vier

Unterkategorien (strategische und organisatorische Risiken, technische Risiken, rechtliche Risiken und nicht-cloud-spezifische Risiken) eingeordnet. Die so ermittelten Sachverhalte konnten durch weitere Recherchen und neu identifizierte Individuen erweitert werden ([BSI10] und [CSA09]). Risiken besitzen eine Eintrittswahrscheinlichkeit („Probability“) und einen Grad der Schwere ihrer Auswirkung („Impact“). Diese, wie auch der wahrgenommene Wert („Value“) eines Assets, werden in der Ontologie auf einer Skala mit fünf Punkten bewertet. Risiken besitzen darüber hinaus eine Verbindung zu der Klasse „ParkerianHexad“, um eine Zuordnung der in [Par02] aufgestellten Kriterien der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit, Besitz/Kontrolle, Authentizität und Nützlichkeit) vorzunehmen.

Sicherheitsmaßnahmen, die zur Absicherung von Cloud-Computing-Diensten genutzt werden können, wurden anhand von Security Whitepaper (Vgl. [AWS10], [Goo10] und [Mic10]), [BSI10] sowie [CSA09] identifiziert. Auf diese Weise konnten insgesamt 77 Sicherheitsmaßnahmen in 9 Kategorien in die Ontologie aufgenommen werden. In der nachfolgenden Tabelle 1 sind neben den Kategorien die Anzahl der Sicherheitsmaßnahmen und Beispiele dargestellt.

Kategorie	**Anzahl Sicherheitsmaßnahmen**	**Beispiele für Sicherheitsmaßnahmen**
Change Management	4	Review, Test and Approval of Hardware Changes; Software Updates without Service Interruption
Compliance and Legal	8	Intellectual Property resides with Customer; Legal Review of Request for Information Disclosure
Data Security	20	Encrypted Key Exchange; Safe Disposal of Storage Devices
Economic Security	5	Source Code Escrow; Optional Resource Capping
Employee Security	7	Background Checks; Periodical Permission Review
Failover	6	Redundant Power Supply; Compatibility to other Cloud Services of Different Providers
Incident Management	5	24/7/365 Incident Response; Defined Incident Handling Processes
Network Security	11	Strong Resource Isolation; Encrypted Internal Communication
Physical Security	11	Disaster Management Plan; Multi-Factor Authentication for Physical Access

Tabelle 1: Sicherheitsmaßnahmen für das Cloud Computing

Die Sicherheitsmaßnahmen können vom Anbieter für alle oder nur für ausgewählte Dienste ergriffen werden. Wird eine Maßnahme für alle ergriffen, so wird dies durch die Beziehung zwischen den Klassen „Provider“ und „SecurityMeasure“ erfasst, wohingegen Einzelmaßnahmen über die Beziehung zwischen den Klassen „Service“ und „SecurityMeasure“ erfasst werden. Eine zeitgleiche Erfassung einer Sicherheitsmaßnahme für einen Dienst und dessen Anbieter wäre redundant und ist somit zu vermeiden.

Die Kategorisierung der Dienste wurde anhand der OpenCrowd Cloud Taxonomy (http://cloudtaxonomy.opencrowd.com) vorgenommen. Die Dienste werden so auf zwei Ebenen kategorisiert: Einmal auf der Ebene der Dienstmodelle (also SaaS, PaaS und IaaS), wie sie auch in [YBS08] und [OBM10] vorgeschlagen werden, und auf einer

darunter liegenden Ebene, die eine Unterscheidung nach Dienstzweck vornimmt (bspw. CRM-, ERP- oder Dokumentmanagement-Software als Untergruppen von SaaS). Die genutzte OpenCrowd Cloud Taxonomie nennt zusätzlich noch „Cloud Software“ als vierte Gattung. Diese liegt jedoch außerhalb der Betrachtungen dieser Arbeit, da darin Software und Dienste aufgeführt werden, die dazu genutzt werden um eigene Cloud-Computing-Dienste zu implementieren oder bereits in Anspruch genommene zu managen oder zu überwachen, und somit keine eigenständigen Cloud-Computing-Dienste darstellen.

Bei der Betrachtung des Sicherheitsmanagements eines Anbieters ist es sinnvoll zu untersuchen, welche für die IT-Sicherheit relevanten Zwischenfälle es in der Vergangenheit gegeben hat; zu diesem Zweck wurde die Klasse „Incident“ (Zwischenfälle) eingefügt. Zwischenfälle werden in die in [SGM08] dargelegten Kategorien eingeordnet und anhand ihrer Rahmendaten, wie z. B. Zeitpunkt, Dauer und einer Beschreibung, erfasst. Zwischenfälle sind dabei als Eintreten bestimmter Risiken aufzufassen. Wenn also eine DDoS-Attacke zu einem Ausfall eines Dienstes führt, dann ist dies ein Eintreten des Risikos einer DDoS-Attacke. Der Übersichtlichkeit halber wurde die Klasse „Risk“ ein zweites Mal in die Abbildung 1 eingefügt, in der Ontologie selbst liegt sie jedoch nur einmal vor. Ebenso wurden die Kategorien der Zwischenfälle nicht mit in die Grafik aufgenommen.

Zwischen dem Komplex der Anbieter, Dienste und der Sicherheitsmaßnahmen bestehen drei Verbindungen, die die nachfolgenden Fragestellungen beantworten können:

- Welche Sicherheitsmaßnahmen werden von den Anbietern für welche Dienste ergriffen um ihn abzusichern?
- Welche Sicherheitsmaßnahmen sollten von den Anbietern für welche Dienste ergriffen werden um ihn abzusichern?
- Welche Sicherheitsmaßnahmen hätten einen Zwischenfall weiter abschwächen oder sogar verhindern können?

Um die zweite Frage beantworten zu können, wurde festgelegt, welche Schwächen für welche Dienstkategorie relevant sind. So ist es bspw. unwahrscheinlich, dass eine Sicherheitslücke im Hypervisor eines SaaS-Angebots ausgenutzt werden kann, um Daten anderer Kunden auszuspähen, wohingegen dies bei einem IaaS-Angebot aufgrund der Nähe zur Infrastruktur wahrscheinlicher ist.

7 Implementierung

7.1 Technische Umsetzung

Die Implementierung einer Oberfläche zur Abfrage der Ontologie wurde in die bestehende Form von CloudServiceMarket.info eingebunden um Synergien zu erzielen und redundante Arbeit zu vermeiden. Da die Website in ASP.net geschrieben wurde, bietet

es sich an das nun zu implementierende Werkzeug ebenfalls in ASP.net zu schreiben. Bisher steht jedoch keine fertige Implementationen von OWL/SPARQL in ASP.net zur Verfügung. Aus diesem Grund erfolgt eine Implementierung in PHP mit Hilfe des Programmierframeworks ARC2 (http://arc.semsol.org), welches Klassen zur Verarbeitung von RDF-Dateien in PHP zur Verfügung stellt. Für die Überführung der OWL-Dateien in die Webanwendung sind verschiedene Zwischenschritte notwendig, da das verwendete Framework ARC2 keine eigenen Inferenzmechanismen besitzt. Aus diesem Grund müssen die in ARC2 zu importierenden OWL-Dateien nicht nur die zugesicherten, sondern auch die abgeleiteten Axiome beinhalten.

7.2 Funktionsumfang

Die Startseite des Prototypen beinhaltet grundlegende Erläuterungen zum Ziel und Funktion der Ontologie. In einem horizontalen Menü können Funktionen zur Abfrage von Individuals, zu vordefinierten Abfragen oder zum SPARQL-Endpoint aufgerufen werden. Um eigene Abfragen mit dem SPARQL-Endpoint erstellen zu können, ist es notwendig die Individuen der Klassen zu kennen. Hierzu wurde die Funktion „Browse Individuals“ implementiert. In Abbildung 3 ist die Grundform für die Abfragen zur Ermittlung der Individuen einer Klasse dargestellt. Die von der Datenbank zurückgegebenen Datensätze werden in tabellarischer Form mit den statischen Überschriften „Label“ und „URI“ ausgegeben. Darunter erfolgt die Ausgabe der genutzten SPARQL-Abfrage.

```
PREFIX cc: <http://www.cloudservicemarket.info/CC-Security.owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
SELECT ?uri ?label
WHERE { ?uri a cc:LegalRisk;
             rdfs:label ?label }
```

Abbildung 3: Einfache SPARQL-Abfrage zum Abruf der Individuals der Klasse "LegalRisk"

Die Implementierung enthält insgesamt 13 vordefinierte Abfragen, damit Benutzer ohne SPARQL-Kenntnisse ebenfalls Zugang zur Ontologie erhalten. In Abbildung 4 ist eine Übersicht dieser Abfragen abgebildet. Die Abfragen werden in Form einer kurzen Beschreibung als Hyperlink dargestellt und bieten einen Überblick der Funktionen und Abfragen. Eine Beschreibung kann abgerufen werden indem der Mauszeiger über einen der Hyperlinks bewegt wird. Daraufhin öffnet sich ein Fenster mit weiteren Informationen. Aufgrund der Komplexität einiger Abfragen wurde jede Abfrage mit Schlagworten versehen, die mit Hilfe der Filterfunktion über der Liste der Abfragen ausgewählt werden können. Durch eine Kombination der Schlagworte können auch komplexe Abfragen schnell identifiziert werden.

ISBN 978-3-88579-286-4

Abbildung 4: Auswahl vordefinierter Abfragen

Das ARC2 Framework stellt einen SPARQL-Endpoint zur Verfügung, der dazu verwendet werden kann SPARQL-Abfragen zu starten. Es mussten jedoch einige Modifikationen vorgenommen werden, um den SPARQL-Endpoint in den Prototypen zu implementieren. Bspw. unterstützt der SPARQL-Endpoint Funktionen, um Daten in die Ontologie zurückzuschreiben; dies ist allerdings nicht erwünscht, da so unbemerkt nicht geprüfte Daten in die Ontologie eingespielt werden können. Aus diesem Grund wurde diese Funktion entfernt.

8 Evaluation

Konzeptuelle Evaluation: Eine konzeptuelle Evaluation der entwickelten Ontologie sowie von CloudServiceMarket.info fand in Form von Experteninterviews begleitend zur Prototypentwicklung statt ([Wal06], [MS95]). Auf diese Weise war es möglich noch während des Entwicklungsprozesses auf Kritik und Verbesserungsvorschläge einzugehen. Nach dem ersten Prototyp, der genutzt wurde, um die betreffende Domäne grob zu

erfassen, wurde der sog. Throw-Away-Ansatz des Prototypings ([Dav92]) verfolgt und die Weiterentwicklung an dem ersten Prototypen zugunsten einer kompletten Neufassung eingestellt. Aufgrund dieses Vorgehens, konnte im weiteren Verlauf ein Prototyp entwickelt werden, der frei von den Altlasten seiner Vorgänger ist. Der zweite Prototyp wurde um einige Funktionen, wie z. B. die Verfügbarkeit der Dienste und die damit verbundene Gutschriften, die zugehörigen Risiken und die Parker'schen Kriterien für die Informationssicherheit ([Par02]) ergänzt. Der auf diese Weise entstandene zweite Prototyp wurde in einem weiteren Experteninterview evaluiert, wobei die Kritik lediglich auf Details gerichtet war, wodurch der dritte und letzte Prototyp evolutionär auf dem zweiten aufbauen konnte.

Evaluation der Implementierung: Die Evaluation der Bedienbarkeit der Implementierung wurde in Form von strukturierten Interviews durchgeführt ([Wal06]). Die zwei Testpersonen fanden schnell Zugang zu der vorgelegten Implementierung und konnten mit wenig Zeitaufwand Ergebnisse aus den vordefinierten Abfragen extrahieren und interpretieren. Die Menüführung und Eingabeaufforderungen empfanden die Probanden als sinnvoll und leicht verständlich. Auch wenn die Testpersonen Kenntnisse der Abfragesprache SQL besitzen, so war ihnen SPARQL bis dahin nicht bekannt. Durch die Ausgabe der SPARQL-Abfragen auf jeder Seite war es ihnen aber schnell möglich, Abfragen, die von einer vordefinierten Abfrage generiert wurden, im SPARQL-Endpoint zu reproduzieren und zu erweitern.

9 Zusammenfassung

9.1 Limitationen und weitere Forschungsarbeit

Die in der Ontologie enthaltenen Dienste und Anbieter sind nur sehr rudimentär erfasst. So fehlen z. B. Angaben über den Unternehmenssitz, Rechtsform oder Gründungsdatum der Anbieterfirmen oder Beschreibungen der Dienste. In zukünftigen Versionen der Ontologie wäre es denkbar, diese Klassen um weitere Eigenschaften zu ergänzen, die diese und ähnliche Sachverhalte abbilden.

Die Ontologie profitiert, wie auch CloudServiceMarket.info, von möglichst zahlreichen Datensätzen. Der Markt für Cloud Computing entwickelt sich jedoch noch und weist ein hohes Innovationspotenzial auf. Dieses wird jedoch auch von Personen geteilt, die an neuen Attacken auf die Cloud-Computing-Dienste arbeiten. Aus diesen Gründen wird es in Zukunft notwendig sein neue Risiken, Schwächen und Sicherheitsmaßnahmen in die Ontologie zu integrieren. Ziel der Plattform ist zukünftig weitere Anbieter und Dienste aufzunehmen, um weiterhin unabhängige Informationen anzubieten. Die Ontologie enthält jedoch derzeit (Juli 2011) nur Dienste von einem geringen Teil der auf CloudServiceMarket.info erfassten Anbieter.

Auch funktional ließe sich der SPARQL-Endpoint verbessern. Besonders bei komplexeren Abfragen wäre das aus Programmierumgebungen bekannte Syntax-Highlighting oder sogar ein grafisches Assistenzsystem ([Hog10]) hilfreich. Die Webanwendung ließe sich

darüber hinaus um eine Schnittstelle erweitern, die es anderen Anwendungen ermöglichen würde auf die enthaltenen Daten zurückzugreifen.

Personen und Organisationen haben unterschiedliche Auffassungen darüber wie die in der Ontologie vorgeschlagenen Assets, Impacts und Probabilities zu bewerten sind, daher wäre es hilfreich den Benutzern diese Kategorisierungen zu ermöglichen.

9.2 Implikationen

Mit der im Rahmen dieser Arbeit erstellten Ontologie bzw. mit CloudServiceMarket.info liegt eine umfangreiche Wissensquelle vor, die Hilfestellung bei der Umsetzung eines Sicherheitsmanagements im Cloud Computing bietet. Die Adressaten der Implementation sind vor allem Anwenderunternehmen. Kunden von Cloud-Computing-Diensten können die Ontologie und ihre Implementation nutzen, um Sicherheitsanforderungen mit den vom Anbieter ergriffenen Sicherheitsmaßnahmen zu vergleichen. Gleichermaßen können Anbieter recherchieren, welche Sicherheitsmaßnahmen von ihren Mitbewerbern getroffen werden, und die eigenen entsprechend anpassen.

Die Verknüpfung von Werten, Risiken, Schwächen und Sicherheitsmaßnahmen bietet auch einen ersten Ansatz zum Risikomanagement im Cloud Computing, so unterstützt die Ontologie z. B. bei der Identifikation von Risiken oder bei der Überprüfung von eingesetzten Sicherheitsmaßnahmen der Anbieter.

Danksagung

Diese Arbeit ist im Rahmen des Projekts "IT-for-Green: Umwelt-, Energie- und Ressourcenmanagement mit BUIS 2.0" entstanden. Das Projekt wird mit Mitteln des Europäischen Fonds für regionale Entwicklung gefördert (Fördernummer W/A III 80119242).

Literaturverzeichnis

[AWS10] Amazon Web Services: Overview of Security Processes. URL: http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf, 8/2010, Abruf: 13.4.2011.

[Arm09] Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.; Katz, R.; Kanwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M.: Above the Clouds – A Berkeley View of Cloud Computing. In: Communications of the ACM, Vol. 53, Nr. 4, 2009, S. 50-58.

[Ber09] Berl, A.; Gelenbe, E.; di Girolamo, M.; Giuliani, G.; de Meer, H.; Dang, M. Q.; Pentikousis, K.: Energy-Efficient Cloud Computing. In: The Computer Journal, Vol. 53, Nr. 7, 2009, S. 1045-1051.

[Bit06] Bitkom: Compliance in IT-Outsourcing-Projekten – Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen. URL: http://www.bitkom.org/de/themen/36129_40787.aspx, 2006, Abruf: 20.4.2011.

[Bro09] Vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search

Process. In (Newell, S.; Whitley, E.; Pouloudi, N.; Wareham, J.; Mathiassen, L. Hrsg.): Information Systems in a Globalising World: Challenges, Ethics, and Practices, Proc. of the 17th European Conference on Information Systems, Verona 2009.

[BSI10] Bundesamt für Sicherheit in der Informationstechnik: BSI-Mindestanforderungen an Cloud-Computing-Anbieter (Entwurf). URL: https://www.bsi.bund.de/cln_183/ ContentBSI/Presse/Pressemitteilungen/Presse2010/Cloud_Computing_28092010.html, 27.9.2010, Abruf: 17.4.2011.

[Cra01] Cranefield, S.: UML and the Semantic Web. In: Proc. Of the International Semantic Web Working-Symposium, Stanford 2001.

[CSA09] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. URL: https://cloudsecurityalliance.org/csaguide.pdf, 12/2009, Abruf: 17.4.2011.

[Dav92] Davis, A. M.: Operational Prototyping: A New Development Approach. In: IEEE Software, Vol. 9, Nr. 5, 1992, S. 70-78.

[Eni09] ENISA: Cloud Computing - Benefits, risks and recommendations for information security. URL: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, 2009, Abruf: 15.4.2011.

[FE09] Fenz, S.; Ekelhart, A.: Formalizing information security knowledge. In: Proc. of the 2009 ACM symposium on information, computer and communications security, Sydney 2009.

[Gen03] Gennari, J. H.; Musen, M. A.; Ferguson, R. W.; Grosso, W. E.; Crubézy, M.; Erikson, H.; Noy, N. F.; Tu, S. W.: The Evolution of Protégé: an environment for knowledge-based systems development. In: International Journal of Human-Computer Studies, Vol. 58, Nr. 1, 2003, S. 89-123.

[Gen08] Gentzsch, W.: Grids are Dead! Or are they?. URL: http://beta.hpcinthecloud.com/hpccloud/2008-06-16/grids_are_dead_or_are_they.html, 16.6.2008, Abruf: 21.4.2011.

[Goo10] Google: Security Whitepaper: Google Apps Messaging and Collaboration Products. URL: http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/de//a/help/intl/en/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf, 2010, Abruf: 13.4.2010.

[GR95] Guttman, B.; Roback, E.: An Introduction to Computer Security: The NIST Handbook. URL: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=890080, 2.10.1995, Abruf: 3.5.2011.

[HS10] Han, T.; Sim, K. M.: An Ontology-enhanced Cloud Service Discovery System. In: Proc. of the International MultiConference of Engineers and Computer Scientists, Hong Kong 2010.

[Hog10] Hogenboom, F.; Milea, V.; Frasincar, F; Kaymak, U.: RDF-GL: A SPARQL-Based Graphical Query Language for RDF. In (Chbeir. R.; Badr, Y.; Abraham, A.; Hassainen, A.-E. Hrsg.): Emergent Web Intelligence: Advanced Information Retrieval, Springer, London, 2010, S.87-116.

[KS10] Kang, J.; Sim, K. M.: An Agent-based Cloud Search Engine that Consults a Cloud Ontology. In: Proc. of the Annual International Conference on Cloud Computing and Virtualization, Singapur 2010.

[KBM08] Kashyap, V.; Bussler, C.; Moran, M.: The Semantic Web, Springer, Berlin, 2008.

[LT09] Liebold, R.; Trinczek, R.: Experteninterview. In (Kühl, S.; Strodtholz, P.; Traffertshofer, A. Hrsg.): Handbuch Methoden der Organisationsforschung – Quantitative und Qualitative Methoden, VS Verlag für Sozialwissenschaften, Wiesbaden, 2009, S. 32-56.

[MS95] March, S. T.; Smith, G. F.: Design and natural science research on information technology. In: Decision Support Systems, Vol. 15, Nr. 4, 1995, S. 251-266.

[MT09] Martens, B.; Teuteberg, F.: Why Risk Management Matters in IT-Outsourcing – A Systematic Literature Review and Elements of a Research Agenda. In (Newell, S.; Whitley,

E.; Pouloudi, N.; Wareham, J.; Mathiassen, L. Hrsg.): Information Systems in a Globalising World: Challenges, Ethics, and Practices, Proc. of the 17th European Conference on Information Systems, Verona 2009.

[MTG11] Martens, B.; Teuteberg, F.; Gräuler, M.: Design and Implementation of a Community Platform for the Evaluation and Selection of Cloud Computing Services: A Market Analysis. In: Proc. of the 19th European Conference on Information Systems, Helsinki 2011.

[MG09] Mell, P.; Grance, T.: The NIST Definition of Cloud Computing, Version 15. National Institute of Standards and Technology, Gaithersburg, 2009.

[Mic10] Microsoft: Windows Azure™ Security Overview V1.01. URL: http://go.microsoft.com/?linkid=9740388, 10.8.2010, Abruf: 13.4.2011.

[Mil09a] Miller, M.: Cloud Computing Pros and Cons for IT Professionals. URL: http://www.informit.com/articles/article.aspx?p=1325269, 24.2.2009, Abruf: 19.4.2011.

[Mil09b] Miller, M.: Cloud Computing Pros and Cons for End Users. URL: http://www.informit.com/articles/article.aspx?p=1324280, 13.2.2009, Abruf: 19.4.2011.

[mOS11] mOSAIC Project: Task T1.2 - Cloud ontology and ontological resource representation. URL: http://www.mosaic-cloud.eu/index.php?option=com_dotprojectquery&view=taskdetail&taskid=8&Itemid=81, 2011, Abruf: 19.4.2011.

[OBM10] de Oliveira, D.; Baião, F. A.; Mattoso, M.: Towards a Taxonomy for Cloud Computing from an e-Science Perspective. In (Antonopoulos, N; Gillam, L. Hrsg.): Cloud Computing: Principles, Systems and Applications, Springer-Verlag, London, 2010; S. 47-62.

[Par02] Parker, D. B.: Toward a New Framework for Information Security. In (Bosworth, S.; Kabay, M. E., Hrsg.): The Computer Security Handbook, 4. Aufl., John Wiley & Sons, New York, 2002, S. 116-136.

[PwC10] PriceWaterhouseCoopers: Cloud Computing – Navigation in der Wolke. URL: http://www.pwc.de/de/prozessoptimierung/trotz-einiger-bedenken-der-virtuellen-datenverarbeitung-gehoert-die-zukunft.jhtml, 10/2010, Abruf: 21.4.2011.

[Ris09] Ristenpart, T.; Tromer, E.; Shacham, H.; Savage, S.: Hey, You, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proc. of the 16th ACM conference on Computer and communications security, Chicago, 2009.

[SGM08] Scarfone, K.; Grance, T.; Masone, K.: Computer Security Incident Handling Guide, Rev. 1. National Institute of Standards and Technology, Gaithersburg, 2008.

[Sin10] Singer, O.: Aktueller Begriff: Cloud Computing. In: Datenschutz und Datensicherheit, Deutscher Bundestag, Berlin, 2010.

[TKF10] Takahashi, T.; Kadobayashi, Y.; Fujiwara, H.: Ontological Approach toward Cybersecurity in Cloud Computing. In: Proc. of the 3rd International Conference on Security of Information and Networks, Taganrog, 2010.

[Wal06] Walsham, G.: Doing Interpretive Research. In: European Journal of Information Systems, Vol. 15, Nr: 3, 2006, S. 320-330.

[WW02] Webster, J.; Watson, R. T.: Analyzing the past to prepare for the future: Writing a literature review. In: MIS Quarterly, Vol. 26, Nr. 2, S. 13-23.

[Wei09] Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T.; Michalk, W.; Stößer, J.: Cloud Computing–A Classification, Business Models, and Research Directions. In: Business and Information Systems Engineering (BISE), Vol. 1, Nr. 5, S. 343-356.

[WH06] Wilde, T.; Hess, T.: Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung. Ludwig-Maximilians-Universität, München, 2006.

[W3C09] World Wide Web Consortium: OWL 2 Web Ontology Language Document Overview. URL: http://www.w3.org/TR/owl2-overview, 27.10.2009, Abruf: 21.4.2011.

[YBS08] Youssef, L.; Butrico, M.; da Silva, D.: Toward a Unified Ontology of Cloud Computing. In: Proc. Grid Computing Environments Workshop, Austin 2008.