Innovative Architektur für sicheres Cloud Computing: Beispiel eines Cloud-Ecosystems im Gesundheitswesen

Mathias Slawik, Sebastian Zickau, Dirk Thatmann, Jonas Repschläger
Tatiana Ermakova, Axel Küpper, Rüdiger Zarnekow

Technische Universität Berlin
Straße des 17. Juni 135
10623 Berlin

Abstract: Der vorliegende Artikel stellt eine innovative Cloud Computing-Architektur vor, die eine Reihe von Herausforderungen im Einsatz von Cloud Computing adressiert: Datensicherheit, Konformität mit rechtlichen und organisatorischen Richtlinien sowie die Interoperabilität von Cloud-Lösungen. Diese ungelösten Herausforderungen bewirken, dass in vielen Branchen mit umfangreichen Anforderungen die Hauptvorteile von Cloud Computing, also Kostenreduzierung und höhere Flexibilität, nicht genutzt werden können. Besonders deutlich wird dies am Beispiel des Gesundheitswesens, wo es einen hohen Bedarf an sicheren und rechtskonformen Cloud Computing-Lösungen gibt. Zum Abschluss des Artikels wird die Evaluierung der vorgestellten Cloud Computing-Architektur im Rahmen des TRESOR Forschungsprojekts dargestellt. Im TRESOR Projekt werden ausgewählte medizinische Anwendungsfälle unter Nutzung dieser Architektur, eingebettet in ein Cloud Computing-Ecosystem, realisiert.

1 Einführung: Motivation, Zielstellung und Aufbau

Das Gesundheitswesen gehört mit 4 Mio. Arbeitnehmern in Deutschland zu den größten Branchenarbeitgebern [Mer08]. Aufgrund von steigenden technischen Ansprüchen wird die Unterstützung der medizinischen Leistungserstellung durch IuK-Systeme und Dienstleistungen zunehmend wichtiger, jedoch sind Ressourcen für Investitionen begrenzt [BW12]. Der Bereich ist geprägt von einer Reihe kleiner und mittelständischer regionaler Unternehmen wie Arztpraxen und Krankenhäusern, welche über eigene, meist jedoch untereinander inkompatible, IT-Infrastrukturen verfügen. Deren Betrieb ist häufig aufwändig und kostenintensiv. Zudem sind hohe Standards bezüglich Datenschutz, Datensicherheit und Rechtskonformität sowie hohe Anforderungen an Interoperabilität, Skalierbarkeit und Verfügbarkeit zu gewährleisten [BW12]. Gerade im Gesundheitswesen existieren kritische Systeme, für die Ausfallzeiten nicht toleriert werden, was einen zusätzlichen Realisierungsaufwand bedeutet. Zusätzlich unterliegt das Gesundheitswesen vielen Reglementierungen und besonderen gesetzlichen Anforderungen [BW12].

Aufgrund der dargestellten Thematik setzt sich der Gesundheitssektor verstärkt mit Alternativen für die Realisierung von IuK-Lösungen auseinander. Eine Möglichkeit, den Herausforderungen zu begegnen, ist eine Verlagerung bestehender medizinischer Informati-

onssysteme in die Cloud. Mit Hilfe von Cloud-Technologien lassen sich Ressourcen wie Rechenleistung, Speicher und Anwendungen auslagern und über das Internet bei Bedarf „as a Service“ abrufen. Cloud Computing hat in den vergangenen Jahren einen Strukturwandel im IKT-Sektor eingeleitet, der Kostensenkungen in Nutzung und Betrieb von Diensten ermöglicht und daher zukünftig im Gesundheitswesen eine Alternative darstellen kann. Daneben bietet das Cloud Computing noch weitere Vorteile, z.B. eine bessere Skalierbarkeit und dadurch höhere Performanz, eine größere Verfügbarkeit, globale Zugriffsmöglichkeiten mit niedriger Latenz und die Möglichkeit der flexiblen Abrechnung von IT-Ressourcen nach Bedarf ([MSEW11], [IH10]). Hierdurch kann eine allgemeine Verbesserung der Dienstqualität für Anwender im stationären und Außendienst realisiert werden [BW12].

Beim Einsatz von Cloud Computing gilt es, grundlegende Herausforderungen zu bewältigen: Es besteht in der Regel die Gefahr einer hohen Abhängigkeit des Kunden vom jeweiligen Cloud-Anbieter, z.B. durch Nutzung proprietärer APIs und Standards, was als *Lock-In-Effekt* bezeichnet wird [CH09]. Darüber hinaus entwickeln sich Cloud-Anwendungen häufig zu ungewollten *Insellösungen*, welche Interoperabilität zwischen unterschiedlichen Plattformen nicht sicherstellen können [Ort11]. Für Kunden und Anbieter stellt sich zudem die Frage, wie die Verlagerung und der Betrieb von Cloud-Anwendungen rechtskonform stattfinden können. Daneben ist das fehlende Vertrauen in existierende Konzepte für Datenschutz und Datensicherheit ein großes Hemmnis für eine schnellere Marktentwicklung in diesem Segment ([BIT09], [KB12]). Darüber hinaus gibt es noch viele ungelöste Problemstellungen besonders bei Cloud-Lösungen für KMUs oder Branchen [Duf12].

Das Ziel dieser Arbeit besteht darin, eine neue Architektur vorzustellen, die vertrauenswürdiges und interoperables Cloud Computing ermöglicht und dadurch dem Kunden die notwendige IT-Sicherheit und Konformität mit rechtlichen Vorgaben und Unternehmensrichtlinien ohne Lock-In-Effekte gewährleistet. Der vorliegende Artikel ist wie folgt aufgebaut: Im zweiten Kapitel werden die Komponenten der Cloud-Architektur vorgestellt und ihre Einbindung in das Cloud-Ecosystem erläutert. Abschnitt 3 stellt verschiedene Anwendungsszenarien im Gesundheitswesen beispielhaft dar und zeigt eine mögliche Realisierung unter Nutzung der Komponenten der vorgestellten Cloud-Architektur. Abschließend werden die Ergebnisse zusammengefasst und ein Ausblick auf die kommenden Forschungstätigkeiten gegeben.

2 Cloud-Architektur

Durch den Einsatz von Cloud Computing verändert sich die Bereitstellung und die Nutzung von Diensten. Vorteilen, wie z.B. der besseren Skalierbarkeit von Diensten, stehen jedoch auch eine Vielzahl an neuen Sicherheitsrisiken gegenüber, denen begegnet werden muss [BS12]. Im Bereich technischer und administrativer Maßnahmen zur Absicherung von Cloud Computing-Umgebungen existieren bereits einige Ansätze [Win11] [KV10]. Jedoch befinden sich im Bereich von Datenschutz, rechtlichen Grundlagen von Cloud Computing, Cloud Computing in KMUs und in branchenspezifischen Cloud-Anwendungen aktuelle Herausforderungen und ungelöste Fragestellungen [Duf12].

Die in diesem Artikel vorgestellte Cloud-Architektur soll einige dieser Herausforderungen, zusammengefasst unter den Begriffen *Sicherheit*, *Konformität* und *Interoperabilität*, durch einen neuen Lösungsansatz adressieren:

- Der Bereich *Sicherheit* ist innerhalb von Cloud Computing-Architekturen ein wichtiges Querschnittsthema. Zu diesem Thema gehören eine Vielzahl an Technologien, unter anderem aus den Bereichen Authentifizierung, Autorisierung, Identity Management und Security Monitoring. Darüber hinaus müssen auch die jeweiligen Cloud Deployment-Modelle Beachtung finden, beispielsweise die Sicherheit der VM-Hypervisor bei IaaS-Angeboten oder die Sicherheit der Web-Oberfläche bei SaaS-Diensten [LTM+11].
- Im Bereich *Konformität* von Cloud Computing existieren viele Unsicherheiten, vor allem in Bezug auf die Einhaltung von Datenschutzgesetzen und unternehmensspezifischen Richtlinien [Rui11].
- Neben diesen beiden Schwerpunkten soll die Cloud-Architektur *Interoperabilität* mit Hilfe offener Standards erreichen und somit *Lock-In-Effekte* und *Insellösungen* vermeiden.

Die Anwendbarkeit wird durch die prototypische Realisierung von Cloud-Lösungen für branchenspezifische (d.h. medizinische) Anwendungsfälle in einem mittelständischen Umfeld der Gesundheitsbranche gezeigt.

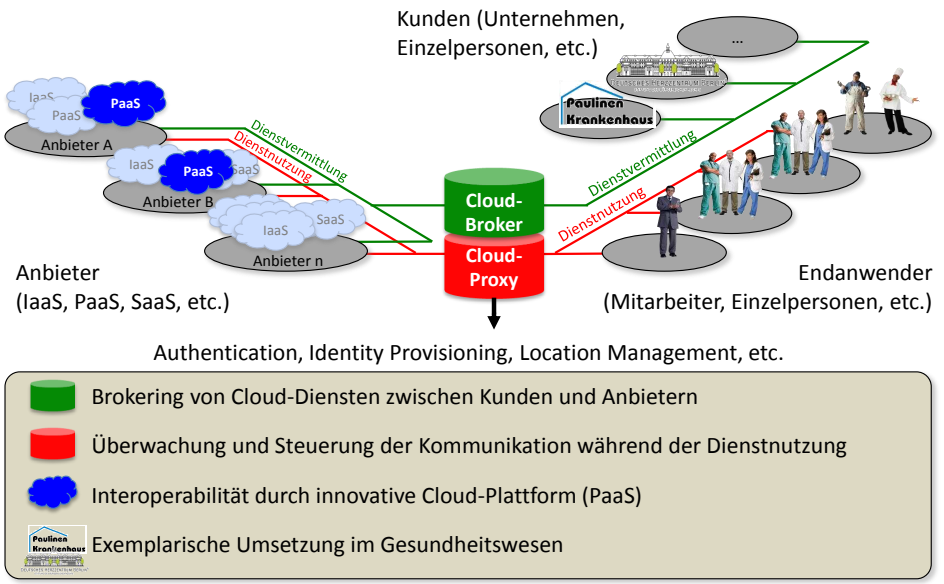

Abbildung 1: Darstellung der Cloud-Architektur

Der zentrale innovative Ansatz der Cloud-Architektur ist die Einführung eines *Cloud-Proxys* als neues Architekturelement. Jedwede Kommunikation zwischen Endanwendern und Cloud-Diensten (*IaaS*, *PaaS* und *SaaS*) wird durch den Cloud-Proxy geführt.

Diese Architektur-Bedingung ermöglicht dem Cloud-Proxy einerseits die Überwachung und Kontrolle des Kommunikationsflusses und dadurch die Sicherstellung von Konformitätsanforderungen. Andererseits können über den Cloud-Proxy übergreifende Funktionalitäten im Bereich *Sicherheit* bereitgestellt werden. Dazu gehören offensichtliche, wie z.B. einheitliche Authentifizierung und Identitätsmanagement, aber auch innovative Funktionen, beispielsweise ortsbasierte Autorisierung von Cloud-Endanwendern.

Eine weitere Architekturbedingung ist die Einführung einer formalen Beschreibung aller Cloud-Dienste innerhalb des Cloud-Ecosystems. Dabei geht die zu schaffende Beschreibungssprache über die gängigen Ansätze, wie WSDL [Con07] oder USDL [Res11], hinaus und wird zusätzlich die Formalisierung von Sicherheits- und Konformitätsbestimmungen ermöglichen. Dies ermöglicht einerseits die Überwachung des Kommunikationsflusses auf Einhaltung dieser formalisierten Bestimmungen durch den Cloud-Proxy zur Laufzeit. Darüber hinaus wird auch das *Brokering* zwischen potentiellen Klienten und Anbietern, sowie das *Matching* zwischen den Klienten-Anforderungen und den Cloud Service-Zusicherungen ermöglicht.

Dieses Brokering und Matching wird durch einen *Cloud-Broker* realisiert. Dieser enthält zwei Repositories: das *Service Repository* mit den formalisierten Beschreibungen und Zusicherungen der Cloud Service-Angebote und ferner das *Profile Repository* mit den während der Nutzung zu beachtenden Richtlinien. In dem Maße, wie sich Konformitätsbedingungen formalisieren lassen, wird hierdurch der mitunter sehr aufwändige manuelle Abgleich zwischen Anforderungen und Zusicherungen automatisiert.

Die Einführung einer offenen, OSGi-kompatiblen Cloud-Plattform (PaaS) ermöglicht die Interoperabilität realisierter SaaS-Lösungen innerhalb des Cloud-Ecosystems. Ziel der OSGi-Technologie ist die Förderung der Komponentenorientierung von Softwaremodulen und Applikationen, und damit die Senkung von Softwarekomplexität und die Zusicherung von Interoperabilität von Diensten durch offene Spezifikationen [All12].

3 Einbindung der Cloud-Architektur in das Gesundheitswesen

Mit dem Projekt „TRusted Ecosystem for Standardized and Open cloud-based Resources (TRESOR)“ - gefördert durch das BMWi Förderprogramm Trusted Cloud - wird eine Infrastruktur geschaffen, um Dienste aus der Cloud sicher und vertraulich zu nutzen. Hierbei werden Daten (z.B. Patientendaten) durch strikte Regeln vor unbefugten Zugriffen geschützt und bislang isolierte IT-Systeme auf Basis einer vertrauenswürdigen Plattform in die Cloud eingebunden. Notwendige Ressourcen werden unter Berücksichtigung von Unternehmensrichtlinien und gesetzlichen Vorschriften von einem Cloud-Broker vermittelt, gebündelt und zugänglich gemacht. Die Herausforderungen, mit denen sich Abnehmer und Anbieter auseinandersetzen, liegen einerseits in einem skalierbaren und standardisierten Austausch von IT-Ressourcen und -Diensten zwischen mehreren Akteuren, vergleichbar

mit einem Cloud-Ecosystem ([LBRK10], [BIT09]), und andererseits in einer rechtlichen Absicherung und Gewährleistung der IT-Sicherheit in der Cloud. Für eine vertrauenswürdige Nutzung ist eine Gewährleistung der kundenseitigen Anbieter-Anforderungen sehr wichtig. Dies kann über eine geeignete Cloud-Zertifizierung vom Plattformbetreiber oder externen Akteuren (z.B. BSI oder TÜV) erfolgen. Der EuroCloud Deutschland eco Verband (SaaS Gütesiegel) und das BSI (Sicherheitsempfehlungen für Cloud Computing Anbieter) haben in diesem Zusammenhang bereits erste Zertifizierungs- und Evaluationsvorhaben initiiert.

Die Relevanz und Anwendbarkeit solch eines Cloud-Ecosystems im Gesundheitswesen inkl. PaaS-Plattform und Cloud-Broker im Bereich der Patientenversorgung wird durch das *Deutsche Herzzentrum Berlin* und das *Paulinenkrankenhaus* sichergestellt. Hierbei wurden basierend auf den Experteninterviews eine medienbruchfreie medizinische Verlaufsdokumentation und die Prüfung einer Interaktion von Arzneimitteln im Gesundheitswesen als zentrale Anwendungsfelder im Cloud Computing definiert [BW12]. Diese Beispielszenarien werden zur Verifizierung der Architektur durch das Projektkonsortium realisiert.

Anwendungsszenario 1: Medienbruchfreie medizinische Verlaufsdokumentation
Eine der größten Herausforderungen bei der klinikübergreifenden stationären Versorgung von Patienten ist die Gestaltung einer datenschutzkonformen, geschlossenen und institutsübergreifenden Prozesskette mit einer medienbruchfreien und durchgängigen Verlaufsdokumentation. Von dieser würden die Patienten und die an ihrer Behandlung beteiligten Akteure unmittelbar profitieren. Diese Verlaufsdokumentation ist auch für die Behandlung von Patienten über den stationären Aufenthalt hinaus essentiell, um therapiepflichtige Veränderungen frühzeitig erkennen und entsprechend intervenieren zu können. Bisherige Ansätze skalieren hier nur begrenzt und weisen Probleme hinsichtlich Interoperabilität und Datenschutz auf.

Mit der PaaS-Plattform innerhalb eines Cloud-Ecosystems, welche auf standardisierte Dienstmodelle und Formate zurückgreift, können diese Interoperabilitätsprobleme adressiert werden, während der Cloud-Broker einen für jeden der beiden Partner maßgeschneiderten Zugang unter Berücksichtigung seiner Datenschutzrichtlinien auf die gemeinsam genutzten Cloud-Ressourcen zur Verfügung stellt. Zusätzlicher Mehrwert würde entstehen, wenn weitere Daten (Blutdruck, Gewicht, Eigen- und Fremdbeobachtungen) in ein cloud-basiertes Patientendatenmanagementsystem übernommen, präsentiert, selektiert und über sichere Verbindungen überall und jederzeit abrufbar zur Verfügung gestellt werden könnten. Über diese sicheren Verbindungen könnten Patienten ihre Positionsdaten auf Wunsch freigeben, damit bei medizinischen Problemen zielgerichteter gehandelt werden kann.

Anwendungsszenario 2: Optimierung der medizinischen Behandlungskette am Beispiel der Prüfung von Arzneimittelinteraktionen
Unerwünschte Arzneimittelwirkungen gehen häufig auf nicht abgestimmte Medikamentenkombinationen und –dosierungen zurück und spielen in der Patientenversorgung eine wesentliche Rolle bei der Komplikationsrate und Mortalität. Ausschlaggebend für das Auftreten solcher Probleme sind auch demographische und klinische Daten des Patienten, zum Beispiel Alter, Geschlecht, Gewicht, Körperoberfläche, Allergien sowie Nieren- und Leberfunktionen. Auch treten entlang des Behandlungsprozesses häufig komplexe Fragestellungen auf, die abhängig sind von zu spezifizierenden Attributen wie Diagno-

sen, Pflegediagnosen, Prozeduren und anderen medizinischen Daten. Sie können mittels Leitlinien, Pflegerichtlinien, Fachinformationen und wissenschaftlichen Publikationen beantwortet werden. Zum Aufzeigen unerwünschter Arzneimittelinteraktionen oder weiterer Informationsangebote werden heute in der Regel lokal installierte Informationssysteme verwendet, deren Datenbestand aufwändig und meist zeitverzögert aktualisiert wird und die darüber hinaus den Nachteil haben, dass bei der Eingabe der erwähnten Patientendaten häufig Medienbrüche vorkommen.

Ein Cloud-Ecosystem, welches unterschiedlichen Akteuren wie Krankenhäusern, Arztpraxen und Apotheken Zugriff auf Arzneimittelinteraktionsdatenbanken und weitere personalisierte Informationen gibt, kann diese Probleme beheben. Angedacht ist die Etablierung eines cloud-basierten Informationsdienstes zur Arzneimittelinteraktionsprüfung, welcher von lokal installierten medizinischen Systemen aufrufbar ist und der mit anderen Anwendungsdiensten des Cloud-Ecosystems, zum Beispiel zum anonymisierten Zugriff auf Patientendaten, orchestriert werden kann. Der Zugriff auf diesen Informationsdienst durch die verschiedenen Akteure wird durch den Cloud-Broker gesteuert und kontrolliert.

4 Fazit und Ausblick

Das neue Paradigma Cloud Computing verändert die Bereitstellung und Nutzung von IT-Diensten. Damit einhergehend entstehen zahlreiche Vorteile, insbesondere Kosteneinsparungen und Flexibilitätssteigerungen. Allerdings existieren in einigen Anwendungsfeldern, insbesondere im Gesundheitswesen, hohe Anforderungen (u.a. Datenschutz, Rechtskonformität), deren Erfüllung eine Herausforderung darstellt. Diese Arbeit stellt Ansätze vor, wie diesen Herausforderungen begegnet werden kann und ermöglicht es dem Gesundheitswesen die Vorteile des Cloud Computings zu nutzen. Die Entwicklung eines generischen Cloud-Ecosystems ermöglicht eine flexible Verwendung auch in anderen Branchen.

Die praktische Tragfähigkeit der Forschungsergebnisse wird durch die Implementierung aller Architekturelemente geprüft. Die TRESOR-Architektur besteht aus einer OSGi-konformen Plattform, die durch Verwendung offener Standards Lock-In-Effekte vermindert. Der Cloud-Proxy überwacht und steuert den Kommunikationsfluss. Der Cloud-Broker vermittelt zwischen Nutzern und Anbietern. Im Projekt kooperieren Partner aus Wirtschaft, Gesundheitswesen und Forschung. Durch diese Zusammenarbeit können innovative Konzepte, wie z.B. Location-based Access Control, im Cloud-Kontext erprobt werden.

Das Cloud-Ecosystem ermöglicht es Anbietern von Diensten neue Geschäftsfelder, in denen Cloud-basierte Lösungen noch nicht realisierbar sind, zu erschließen. Die zu erwartende Kosteneinsparung führt zu einer Freisetzung von Resourcen, die beispielsweise für die Verbesserung der Patientenversorgung genutzt werden kann. Die Entwicklung des Internets der Dienste wird durch die einheitliche Dienstbereitstellung im Ecosystem gefördert.

Literatur

[All12] OSGi Alliance. OSGi Alliance — About / HomePage. http://www.osgi.org/About/HomePage, 2012.

[BIT09] BITKOM. Cloud Computing - Evolution in der Technik, Revolution im Business. BITKOM-Leitfaden. http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf, 2009.

[BS12] Rohit Bhadauria und Sugata Sanyal. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. http://arxiv.org/abs/1204.0764v1, 2012.

[BW12] Wolfgang Bröcker und Joseph Walenta. Experteninterview zum Thema "Motivation Cloud Computing im Gesundheitswesen: Krankenhausperspektive"mit Wolfgang Bröcker (Paulinenkrankenhaus Berlin, Leiter EDV) und Joseph Walenta (Deutsches Herzzentrum Berlin, IT-Projektleiter). http://www.cloud-tresor.de/2012/05/14/experteninterview/, April 2012.

[CH09] Daniele Catteddu und Giles Hogben. Cloud Computing - Benefits, risks and recommendations for information security. Bericht, European Network and Information Security Agency (ENISA), 2009.

[Con07] World Wide Web Consortium. Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. http://www.w3.org/TR/wsdl20/, 2007.

[Duf12] Nicole Dufft. Reality Check Cloud Computing 2012: Wirklichkeit oder Wolkenkuckucksheim? http://www.cloud-practice.de/sites/default/files/downloads/live/07_1000_dufft_pac.pdf, 2012.

[IH10] Bala Iyer und John C. Henderson. Preparing for the future: Understanding the seven capabilities of Cloud Computing. *MIS Quarterly Executive*, 9(2), 2010.

[KB12] KPMG und BITKOM. Cloud Monitor 2012, März 2012.

[KV10] Ronald L. Krutz und Russell Dean Vines. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, Inc., Indianapolis, 2010.

[LBRK10] Stefanie Leimeister, Markus Böhm, Christoph Riedl und Helmut Krcmar. The Business Perspective of Cloud Computing: Actors, Roles and Value Networks. In *The European Conference on Information Systems (ECIS)*, 2010.

[LTM+11] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger und Dawn Leaf. NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505, 2011.

[Mer08] Friedrich Merz. *Wachstumsmotor Gesundheit: Die Zukunft unseres Gesundheitswesens*. Carl Hanser Verlag, München, 2008.

[MSEW11] Günter Müller, Noboru Sonehara, Isao Echizen und Sven Wohlgemuth. Sustainable Cloud Computing. *Business & Information Systems Engineering (BISE)*, 5, 2011.

[Ort11] Sixto Jr. Ortiz. The Problem with Cloud-Computing Standardization. *Computer*, 44(7):13–16, 2011.

[Res11] SAP Research. Was ist USDL und warum brauchen wir es? http://www.internet-of-services.com/index.php?id=264, 2011.

[Rui11] Joep Ruiter. Privacy Regulations for Cloud Computing, Compliance and Implementation in Theory and Practice. In *Computers, Privacy and Data Protection: an Element of Choice*. Springer Science+Business Media, 2011.

[Win11] Vic (J.R.) Winkler. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Elsevier Inc., Waltham, 2011.