# Sicheres Cloud Computing im Gesundheitswesen

Alexander Grzesik [a,1], Torsten Frank [a,1]
[a] medisite Systemhaus GmbH

**Zusammenfassung.** Die Nutzung der Cloud zum Austausch von Daten und dem Einsatz von Programmen hat in den vergangenen Jahren zunehmend an Bedeutung gewonnen. Dies erstreckt sich sowohl über den privaten Bereich, wird in zunehmendem Maße aber auch im wirtschaftlichen Umfeld beobachtet und teilweise bereits produktiv eingesetzt. Dem Einsatz der Cloud im Gesundheitswesen sind dabei im besonderen Maße Einschränkungen und Vorgaben gesetzt, da hier rechtliche Aspekte wie Datenschutz und -sicherheit gesondert beachtet werden müssen. Im Rahmen der Trusted Cloud Initiative [1] des Bundesministeriums für Wirtschaft und Energie (BMWi) soll diesem Umstand mit der gezielten Förderung von drei Cloud-Forschungsprojekten im Gesundheitswesen Rechnung getragen werden. Das Projekt TRESOR – Trusted Ecosystem for Standardized and Open cloud-based Resources – verfolgt dabei als eines der geförderten Projekte den Anspruch, eine offene Cloud-Plattform für das Gesundheitswesen zu schaffen, welche von Beginn an zusammen mit klinischen Anwendern konzipiert wurde und die besonderen Gegebenheiten im Gesundheitswesen berücksichtigt [2].

**Keywords.** Gesundheitswesen, Cloud, PaaS, Datenschutz, Datensicherheit

## Einleitung

Das Internet ist als Bestandteil des Alltags nicht mehr wegzudenken. Wurde es im vergangenen Jahrzehnt primär als Kommunikationsmedium verwendet, gewinnt seit kurzer Zeit zunehmend die Nutzung der durch das Internet nutzbaren Ressourcen an Bedeutung. Insbesondere die Verfügbarkeit von Rechenkapazität und Speicherplatz im Internet hat, verbunden mit zunehmenden Verbindungsgeschwindigkeiten, eine völlig neue Möglichkeit der Nutzung desselben geschaffen. In diesem Zusammenhang wird zunehmend der Begriff der „Cloud“ geprägt, welche eine Kombination der genannten Ressourcen als Infrastruktur im Netz zur Verfügung stellt.

Die Nutzung von Cloud-Infrastrukturen hat sich in den vergangenen Jahren stark verbreitet. Angefangen im privaten Bereich mit Programmen wie Dropbox™ oder den Cloud-Diensten der Google Docs™, bis hin zur Nutzung von Cloud-Infrastrukturen bei rechenintensiven Aufgaben bspw. im universitären Bereich, gewinnt die Cloud zunehmend an Bedeutung und bietet Privatpersonen und vor allem aber auch Firmen und Institutionen eine Alternative gegenüber dem eigenen Vorhalten derartiger Strukturen. Der traditionelle „Server im Keller“ wird zunehmend durch netzbasierte Infrastruktur abgelöst, wobei Faktoren wie Skalierbarkeit und Datenbackup wichtige Kriterien und Argumente sind, eine derartige Struktur zu nutzen.

1 Corresponding Author.

Das Gesundheitswesen steht dezentraler Datenhaltung oder allein dem Transport von Daten über das Internet traditionell eher distanziert gegenüber. In Anbetracht des hohen und schützenswerten Guts der Patientendaten ist dies durchaus auch verständlich, zumal das Patientengeheimnis von hoher Bedeutung im Vertrauensverhältnis zwischen Arzt und Patient ist. Nichtsdestotrotz weisen aber das Internet und vor allem die Möglichkeiten, welche die Nutzung von Cloud-Infrastrukturen bietet, auch wiederum Vorteile auf, deren Nutzung auch im Gesundheitswesen zunehmend erwogen wird.

Das Bundesministerium für Wirtschaft und Energie (BMWi) verfolgt mit der Förderung von Cloud-Forschungsprojekten im Rahmen des Technologieprogramms Trusted Cloud das Ziel der Entwicklung und Erprobung innovativer, sicherer und rechtskonformer Cloud Computing-Lösungen. Von diesen neuen, cloud-basierten Diensten sollen insbesondere mittelständische Unternehmen profitieren. Es werden grundlegende Technologien sowie Cloud-Anwendungen für unterschiedliche Bereiche entwickelt, insbesondere für Industrie, Handwerk, Gesundheit und den öffentlichen Sektor. Die Forschungs- und Entwicklungsaktivitäten haben im September 2011 begonnen und werden bis Anfang 2015 laufen.

## Die TRESOR Architektur

Das Forschungsprojekt TRESOR hat zum Ziel, ein sicheres und datenschutzkonformes Cloud-Ecosystem aufzubauen. Mit dem speziellen Fokus auf das Gesundheitssystem adressiert TRESOR einen Anwendungsbereich, in dem Datenschutz und Datensicherheit von hoher Bedeutung sind und wo vor allem auf gesetzlicher Ebene hohe Hürden und Vorgaben für den Einsatz von Technologie und Telekommunikation gegeben sind [3].

TRESOR konzentriert sich exemplarisch auf Gesundheitseinrichtungen wie etwa Krankenhäuser oder Ärzte aber auch mittelständische und Industrieunternehmen aus dem Gesundheitswesen, da diese Zielgruppen besonders viele Charakteristiken für eine „Trusted Cloud“ aufweisen. So fordert dieser Bereich neben den sehr hohen Standards bezüglich Datenschutz und Datensicherheit aufgrund der Vielzahl der beteiligten Akteure zudem hohe Anforderungen an Interoperabilität, Skalierbarkeit und Verfügbarkeit. Um diesen Anforderungen Rechnung zu tragen, kombiniert die TRESOR Architektur modernste Technologien in einer Infrastruktur, die hohe Skalierbarkeit und Verfügbarkeit mit geprüften Sicherheitsverfahren und Software-Architekturen vereint.

### Überblick über die TRESOR Architektur

Die TRESOR Architektur setzt sich aus vier Hauptkomponenten zusammen:

- Den Schnittstellen für die TRESOR Dienstnutzer
- Dem TRESOR Ecosystem, welches die TRESOR Dienste vermittelt
- Den TRESOR Dienstanbietern, welche ihre Dienste über die TRESOR Plattform den Nutzern zur Verfügung stellen
- Dem IaaS-Anbieter, welcher die Infrastruktur für die TRESOR Plattform zur Verfügung stellt

Aufgrund der modularen Struktur des TRESOR Projektes ist gewährleistet, dass Hauptkomponenten dynamisch gewechselt werden können. Dies kann beispielsweise bedeuten, dass entsprechend Länder-spezifischer Vorgaben verschiedene IaaS-Anbieter die Infrastruktur für Dienstnutzer zur Verfügung stellen. Dies kann ggf. dann notwendig sein, wenn Patientendaten nur innerhalb eines bestimmten Landes gehostet werden dürfen und dafür spezielle Anbieter genutzt werden müssen. Im folgenden Abschnitt werden die einzelnen Komponenten näher beschrieben.

Die Nutzer der TRESOR Dienste im Krankenhaus bemerken gar nicht, dass sie Cloud-Dienste im täglichen Betrieb einsetzen. Dies wird dadurch erreicht, dass die Nutzer diese Dienste nicht direkt aufrufen, sondern diese in die Infrastruktur des Krankenhauses, integriert sind. So sind diese Dienste beispielsweise über Schnittstellen direkt in das Patientendaten-Managementsystem (PDMS) des Krankenhauses integriert. Das PDMS ruft dann im Falle der Nutzung eines Cloud-Dienstes über einen TRESOR-Proxy, diese Dienste auf, wobei Authentifizierung und Autorisierung zur Nutzung des Dienstes automatisch vermittelt werden. So können beispielsweise im Krankenhaus schon vorhandene Benutzerverwaltungssysteme wie ein Active Directory unmittelbar eingebunden werden.

Über den TRESOR Proxy werden nach erfolgter Authentifizierung Cloud-Dienste des TRESOR Ecosystems aufgerufen und die entsprechenden Daten zur Verfügung gestellt, die für die Nutzung der Dienste notwendig sind.

Das TRESOR Ecosystem stellt als zentrale Verwaltungsinfrastruktur alle Komponenten zur Verfügung, die für eine optimale Nutzung der Cloud-Dienste notwendig sind. Dies umfasst zum einen Komponenten für die Verwaltung der Dienste und die Balancierung von deren Auslastung über einen Broker. Zum anderen umfasst das Ecosystem aber auch Komponenten zur Abrechnung der Dienstnutzung sowie Service-Komponenten, die beispielsweise Dienste-Entwicklern Infrastrukturen zum Testen oder Deployment von Anwendungen zur Verfügung stellen.

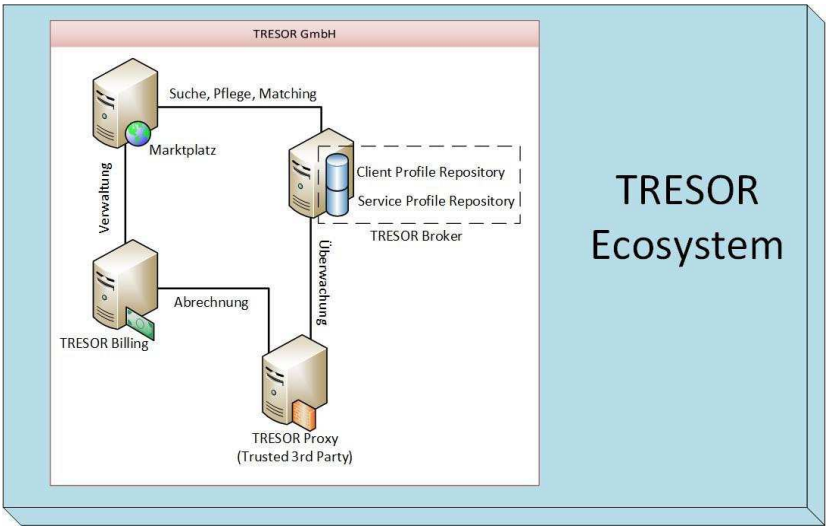


**Abbildung 1.** Das TRESOR Ecosystem

Ein weiterer Kernbestandteil des TRESOR Ecosystems ist eine neue offene PaaS-Plattform (PaaS – Plattform as a Service) für die Bereitstellung und Nutzung standardisierter cloud-basierter System- und Anwendungsdienste, welche an den Cloud Broker als vertrauenswürdigen Mediator zwischen den Klienten und den Cloud-Anbietern des Ecosystems gekoppelt ist.

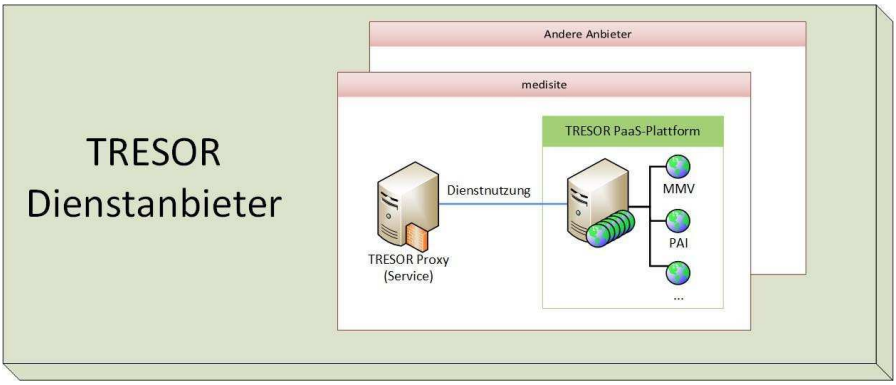


**Abbildung 2.** TRESOR Dienstanbieter

Die PaaS Plattform stellt die Application Server Infrastruktur bereit, in welche die Cloud-Dienste eingestellt werden. Aufgrund der Nutzung offener Standards für die Dienstentwicklung und der Bereitstellung von Entwicklungswerkzeugen wie

beispielsweise APIs aber auch schon umfassender Dienstekomponenten zum Beispiel für Authentifizierung oder Verschlüsselung, ermöglich die PaaS Plattform ein schnelles Bereitstellen neuer Dienste und senkt die Investitionskosten für Dienstanbieter auf ein Minimum, da diese keine eigene technische Infrastruktur zur Entwicklung der Dienste vorhalten müssen. Durch Bereitstellung von dedizierten Testumgebungen wird Dienstanbietern außerdem die Möglichkeit gegeben, mittels frühzeitiger und ggf. auch automatischer Testprozeduren aktuelle Software-Entwicklungsstandards wie testgetriebene Entwicklung im Rahmen des Software Life Cycles zu nutzen, um Dienste sowohl sicher als auch performant zu gestalten.

Die TRESOR Plattform wird von einem IaaS-Anbieter gehostet. Dieser Anbieter stellt die notwendige Infrastruktur zur Verfügung, welche für die Nutzung der Cloud-Dienste notwendig ist.

Der IaaS-Anbieter stellt neben Rechenleistung und Speicherkapazität auch die notwendige Netzwerkstruktur bereit, um dynamisch skalieren zu können und die Erreichbarkeit, jederzeit gewährleisten zu können. Erfordert ein Cloud-Dienst höhere Rechenleistung, kann auf diese Art jederzeit die Rechenleistung durch dynamisches Hinzufügen von Rechenknoten erhöht werden, um eine zügige Bearbeitung der Aufgabe des Dienstes zu ermöglichen.

## Vorteile der TRESOR Plattform

Neben den bereits dargelegten allgemeinen Vorteilen einer Cloud-Infrastruktur wie der dynamischen Skalierbarkeit von Rechenleistung, Speicherkapazität und Netzwerkinfrastruktur weist insbesondere die TRESOR Plattform noch eine Reihe weiterer Vorteile auf, die in diesem Kapitel näher betrachtet werden sollen.

### Sicherheit

Der Schutz von Daten während der Speicherung oder dem Transport über ein Netzwerk ist von hoher Wichtigkeit, und das nicht nur, aber vor allem auch im Gesundheitswesen. Neben den rein rechtlichen Aspekten des Schutzes von Patientendaten sind einem persönlich aber auch die Bedenken vertraut, was eigentlich mit den durch den Arzt bei einer Untersuchung oder der Analyse im Labor erhobenen Daten geschieht und wer Zugriff auf diese hat. Allein die Diskussion um die Einführung der Gesundheitskarte in Deutschland hat sehr deutlich den schmalen Grad in der Balance zwischen Datenschutz und einer effektiven Nutzung und Verfügbarkeit der Patientendaten gezeigt.
Von dieser Diskussion ausgehend stellt sich durchaus die Frage, wie man Daten bei der Nutzung von Cloud-Diensten optimal schützen kann, sodass kein Dritter darauf Zugriff erhält. Diesbezüglich werden Maßnahmen sowohl auf technischer, als auch auf organisatorischer Ebene getroffen.

Auf technischer Seite ist vor allem die Sicherheit der Server und Datenbanken zu gewährleisten. Dies umfasst zum einen die Absicherung der Server und Datenbanken durch aktuell gehaltene (‚gepatchte') Systeme, in welchen Updates zeitnah eingespielt

werden und wo Firewalls und Virenscanner den Zugriff auf Systeme und Daten verhindern oder zumindest erschweren. Ferner wird auf organisatorische Ebene auch der physische Zugriff auf die Infrastruktur kontrolliert. Dies umfasst ein klares Berechtigungskonzept, wer beispielsweise den Serverraum betreten darf, aber auch, wer die Berechtigung zu administrativen Tätigkeiten auf den Servern besitzt.

Auf Seiten der Cloud-Dienste sollten bei der Entwicklung derselben grundlegende Konzepte wie das Prinzip der Datensparsamkeit und die Nutzung von Sicherungsmöglichkeiten der verwendeten Programmiersprache berücksichtigt werden. Dem Prinzip der Datensparsamkeit kommt dabei eine besondere Sorgfaltspflicht zu, welche die Betreiber der TRESOR Plattform in besonderem Maße wahrnehmen. Durch diese wird bei Diensten, welche auf der Plattform zur Verfügung gestellt werden, regelmäßig überprüft, welche Daten zu welchem Zweck genutzt werden.

Einer der wichtigsten Aspekte in Bezug auf Datensicherheit ist allerdings deren Verschlüsselung. Diese soll im Falle, dass Daten doch in falsche Hände geraten, sicherstellen, dass niemand etwas mit den Daten anfangen oder aus diesen Rückschlüsse zum Beispiel auf bestimmte Patienten und deren Krankheiten oder Behandlungen ermöglichen. Um dies zu gewährleisten, werden in TRESOR die Daten vom Client bis zum Server durchgehend verschlüsselt übertragen. Dies umfasst zum einen die medizinischen Daten aber auch Daten, die beispielsweise für die Authentifizierung der Benutzer verwendet werden. Für die Verschlüsselung werden dabei mehrere Verfahren zur Verfügung stehen. Dies ermöglicht es, aufgrund der Vorgaben eines Dienstenutzers (z.B. entsprechend den gültigen Policies in einem Krankenhaus) bestimmte Verschlüsselungsverfahren zum Sichern der Daten zu verwenden.

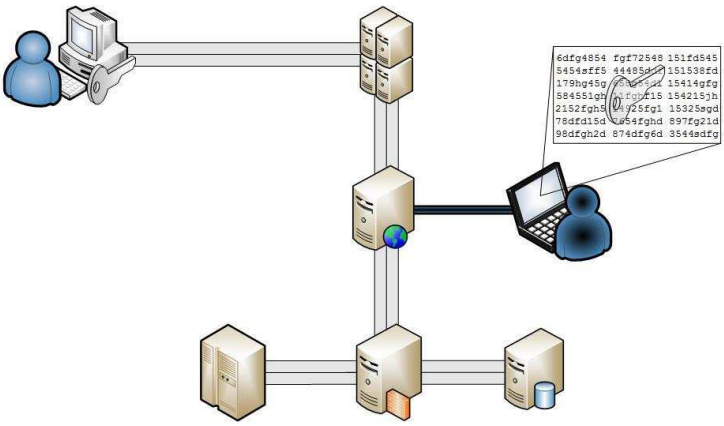


**Abbildung 3.** Durchgehende Verschlüsselung

**Redundanz**

Durch redundante Serverinfrastrukturen in verteilten Rechenzentren ist bei TRESOR jederzeit gewährleistet, dass sowohl gespeicherte Daten als auch Dienste zur Verfügung stehen und dies, auch wenn eines oder mehrere Rechenzentren ausfallen.

Gerade im medizinischen Bereich ist es wichtig, jederzeit auf notwendige Daten eines Patienten oder einer Behandlung zugreifen zu können.

Ein weiterer Vorteil einer redundanten Infrastruktur ist die Möglichkeit, Aktualisierungen von Diensten so zu gestalten, dass der Dienstnutzer davon in der Regel nicht beeinflusst ist. In einer redundanten Cloud-Infrastruktur kann die Aktualisierung knotenweise erfolgen, so dass es für den Benutzer keine Down-Zeiten gibt, in welchen er Dienste oder Daten nicht erreichen kann.

**Lokalisierung von Daten und Diensten**

Bei der Cloud Nutzung stellt sich oft die Frage, wo Daten eigentlich gerade gespeichert werden oder über welche Länder und Standorte diese versandt werden. Insbesondere im Zusammenhang mit medizinischen Daten gelten gesonderte Anforderungen. Entsprechend den Empfehlungen der Europäischen Gemeinschaft [4] und den gesetzlichen Vorgaben über den Datentransfer in Drittstaaten [5] kommt den Standorten von Servern und Datenbanken eine besondere Bedeutung im Rahmen von Cloud-Projekten zu.

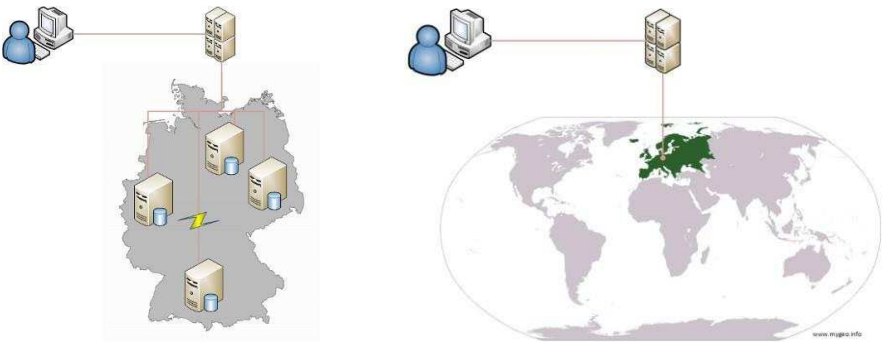

**Abbildung 4.** Redundante Serverstandorte entsprechend den Anforderungen

Das TRESOR Projekt setzt diese Anforderungen von Beginn an um. Der modulare Aufbau der Projekt-Infrastruktur ermöglicht flexible Lösungen, wenn beispielsweise in bestimmten Ländern restriktivere Anforderungen bezüglich der Datenhaltung bestehen. Zum Beispiel im Falle der Schweiz, wo Patientendaten das Land nur verlassen dürfen, wenn die Datenschutzgesetze des Ziellandes mit denen der Schweiz vergleichbar sind, was eine Übertragung von Patientendaten beispielsweise in die USA nur sehr eingeschränkt erlaubt [6,7].

## Anwendungsfälle

Die Umsetzbarkeit der entwickelten Lösungen des Cloud-Ecosystems wird anhand von Anwendungsszenarien aus dem Bereich der Patientenversorgung demonstriert.

Die medienbruchfreie medizinische Verlaufsdokumentation (MMV) ist von hoher Bedeutung insbesondere bei der Verlegung von Patienten zwischen Krankenhäusern. An dieser Stelle bietet ein Cloud-Service zahlreiche Möglichkeiten zur Einsichtnahme von Daten und zum Anpassen (Matching) der Daten von unterschiedlichen Mandanten. Die Nutzung der Cloud bietet hier insbesondere neue Möglichkeiten des Zugriffs auf Daten. So kann im Empfängerkrankenhaus ein Arzt über den Cloud-Dienst Zugriff auf den medizinischen Verlauf des Patienten im anderen Krankenhaus nehmen, um für eine optimale Weiterführung der Behandlung des Patienten zu sorgen. Dies geschieht natürlich nur, wenn die Daten freigegeben wurden und der Arzt bzw. die Pflegekraft die entsprechende Berechtigung zum Zugriff auf diese besitzt.

Beim pharmakologischen Arzneimittel-Interaktionscheck (PAI) wird mittels eines Cloud-Diensts Zugriff auf eine Arzneimittel-Interaktionsdatenbank genommen, um zu überprüfen, ob Wechselwirkungen zwischen angeordneten Medikamenten vorliegen. Ein Vorteil eines Cloud-Dienstes ist hier die Möglichkeit des Zugriffs auf tagesaktuelle Daten, die von den Datenbankbetreibern zur Verfügung gestellt wurden und bisher manuell in den Datenbestand des Krankenhauses eingepflegt werden müssen.

## Zusammenfassung

Mit den beteiligten Projektpartner - der medisite Systemhaus GmbH, der T-Systems International GmbH, der bitplaces GmbH, der TU-Berlin, dem Deutschen Herzzentrum Berlin und dem Paulinenkrankenhaus Berlin - stellt TRESOR ein interdisziplinäres Kooperationsprojekt dar. Es wird erstmals eine "Trusted Cloud" - Infrastruktur bereitstellt, die in der Lage ist, alle relevanten gesetzlichen Vorschriften, Sicherheits- und Datenschutzrichtlinien sowie individuelle Richtlinien mittelständischer Unternehmen und des öffentlichen Sektors zu berücksichtigen. Die **exemplarische** Umsetzung für den Anwendungsbereich der Patientenversorgung wird zukunftsweisend für die weitere Entwicklung von Cloud Services im Gesundheitswesen sein.

### Referenzen


[1] Trusted Cloud Projekt des BMWi, http://www.trusted-cloud.de/ (07.05.2013)
[2] TRESOR Homepage des BMWi, http://www.trusted-cloud.de/de/1690.php (07.05.2013)
[3] Patientenrechtegesetz §630 BGB
[4] Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr 95/46/EG
[5] §§ 4b, 4c BDSG
[6] Art. 6 DSG CH
[7] Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)