

Trusted Cloud im Gesundheitswesen mit TRESOR

Trusted Cloud in healthcare IT with TRESOR

Sebastian MOLL^{a,*}, Torsten FRANK^{a,*}
^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 Technologie (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].

Abstract. The usage of Cloud technologies for data exchange as well as the capability of programs to be run in the Cloud brought this internet-based technology a gain of importance in the last years covering the private customer as well as the industry. With sight on the healthcare sector, the Cloud is confronted with special requirements on data security during storage and transfer leading to the need to address customer concerns respecting privacy in much more detail than other areas. To advance the research on the usage of Cloud technologies in the healthcare sector as well as to enrich discussions on this theme, the German ministry for economy and technology funds three healthcare research projects as part of the Trusted Cloud initiative [1]. The TRESOR – Trusted Ecosystem for Standardized and Open cloud-based Resources – project as one of these three projects has the aim to provide an open platform for Cloud applications for the health care sector [2]. In this project, the clinical users of the platform are involved from the very beginning, allowing to address their requirements and considerations at any time during project progress.

Keywords. Gesundheitswesen, Cloud, Plattform, Datenschutz, Datensicherheit

* Corresponding Author.

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.

Das Gesundheitswesen steht dezentraler Datenhaltung oder allein dem Transport von Daten über das Internet traditionell eher distanziert gegenüber. In Anbetracht des hohen und schätzenswerten 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 Technologie (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. Das Programm Trusted Cloud wurde im September 2010 als Technologiewettbewerb des BMWi ausgeschrieben. Insgesamt haben 116 Projekte an der Ausschreibung teilgenommen. In einem mehrstufigen Prozess mit Unterstützung einer unabhängigen Expertenjury wurden 14 zu fördernde Projekte ausgewählt. An den 14 Projekten sind insgesamt 36 Unternehmen verschiedener Branchen, 27 wissenschaftliche Einrichtungen und vier weitere Institutionen beteiligt. 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. Das Technologieprogramm Trusted Cloud ist der zentrale Beitrag des BMWi zur Umsetzung des Aktionsprogramms Cloud Computing.

Das Forschungsprojekt TRESOR als eines der vom BMWi im Rahmen des Trusted Cloud Programms geförderten Projekte hat den Aufbau eines sicheren und datenschutz-konformen Cloud-Ecosystems zum Ziel, welches exemplarisch für den Anwendungsbereich der Patientenversorgung im Gesundheitswesen umgesetzt wird. Es stellt damit eines von drei aus dem Gesundheitswesen geförderten Projekten des Trusted Cloud Programms dar.

1. 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 auch auf gesetzlicher Ebene hohe Hürden und Vorgaben für den Einsatz von Technologie und Telekommunikation gegeben sind [3].

Das Projekt TRESOR konzentriert sich exemplarisch auf Gesundheitseinrichtungen wie etwa Krankenhäuser oder Ärzte aber auch mittelständische und Industrieunternehmen aus dem Gesundheitswesen, beispielsweise aus dem Pflegebereich, 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 Projekt-Architektur modernste Technologien in einer Infrastruktur, die hohe Skalierbarkeit und Verfügbarkeit mit geprüften Sicherheitsverfahren und Software-Architekturen vereint.

1.1 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.

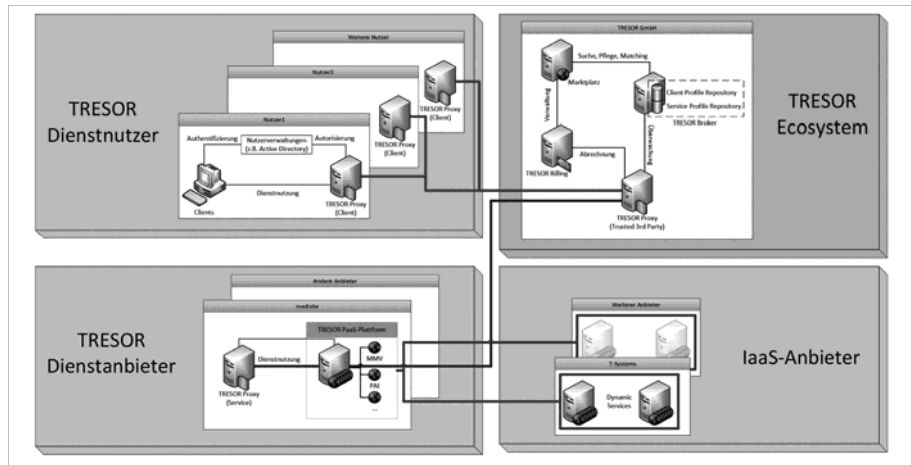


Abbildung 1. Übersicht über die TRESOR Komponenten

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.

1.2 Komponenten der TRESOR Architektur

Die TRESOR Projektarchitektur setzt sich aus vier Hauptkomponenten zusammen (siehe 1.1). Das Zusammenspiel von Dienstnutzern, welche über das Ecosystem Dienste einsetzen, die auf einer IaaS-Infrastruktur gehostet sind, ermöglicht zum einen den gezielten und optimalen Einsatz verfügbarer Ressourcen, zum anderen ermöglicht es Variabilität in hohem Maße, begonnen mit einer Vielzahl unterschiedlicher Dienste, die Nutzern zur Verfügung stehen bis hin zu zahlreichen Skalierungsmöglichkeiten beispielsweise in Hinsicht auf Speicherplatz und Rechenkapazität, aber auch verfügbare Verschlüsselungstechnologien oder beispielsweise die Möglichkeit, verschiedene IaaS-Dienste (IaaS – Infrastructure as a Service) zu nutzen, wenn dies sinnvoll bzw. erforderlich ist.

Die Nutzer der TRESOR Dienste im Krankenhaus bemerken idealerweise 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, mit welcher die Nutzer täglichen Umgang haben, 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, an welchen das System gekoppelt ist, 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.

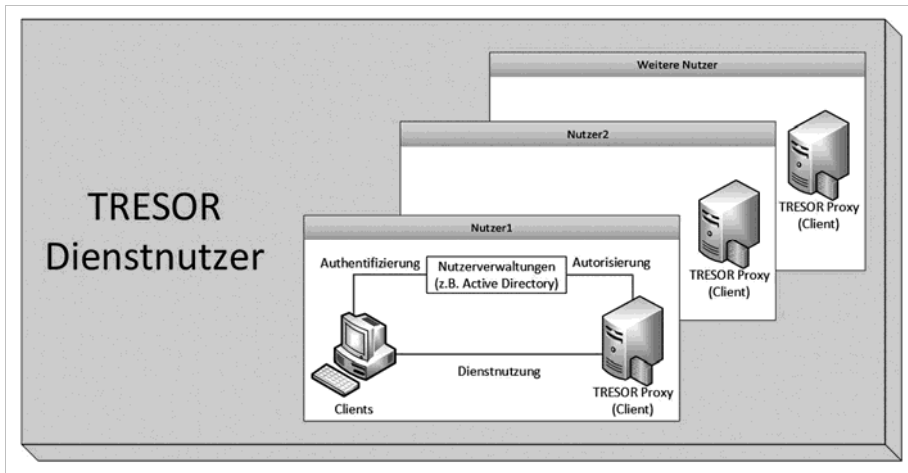


Abbildung 2. TRESOR Dienstnutzer

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.

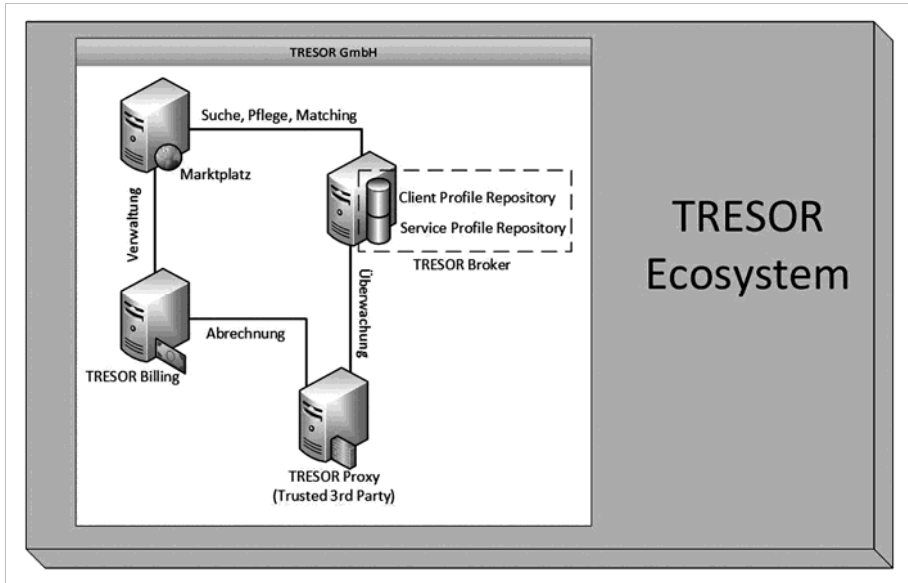


Abbildung 3. Das TRESOR Ecosystem

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.

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, ermöglicht 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 Dienst Anbietern 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.

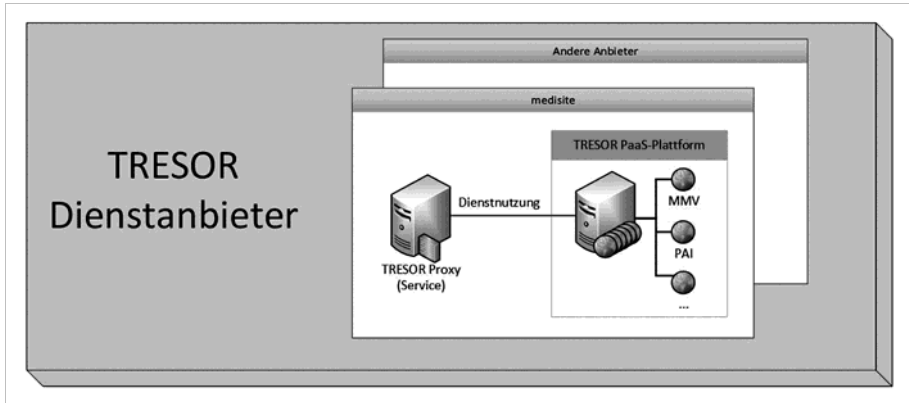


Abbildung 4. TRESOR Diensteanbieter

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.

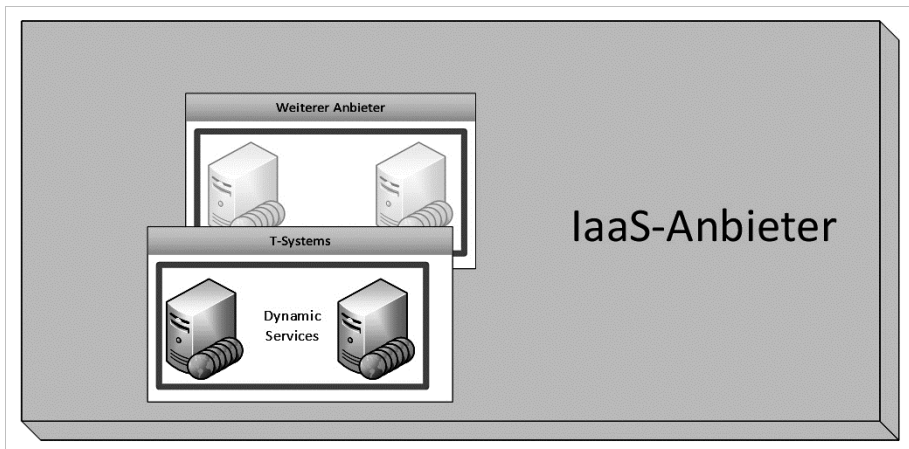


Abbildung 5. TRESOR IaaS -Anbieter

Der IaaS-Anbieter stellt neben Rechenleistung und Speicherkapazität auch die notwendige Netzwerkstruktur bereit, um beispielsweise im Fall hoher Last dynamisch skalieren zu können und die Erreichbarkeit, welche gerade im Gesundheitswesen von hoher Bedeutung ist, jederzeit gewährleisten zu können. Diese Skalierung umfasst aber nicht nur die Netzwerkinfrastruktur, sondern vor allem auch Serverkapazitäten und die Verfügbarkeit von Speicherkapazität. 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.

2. 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.

2.1 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 Virens Scanner den Zugriff auf Systeme und Daten verhindern oder zumindest erschweren. Ferner wird auf organisatorischer 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 (z. B. Java) 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 ziehen kann. 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.

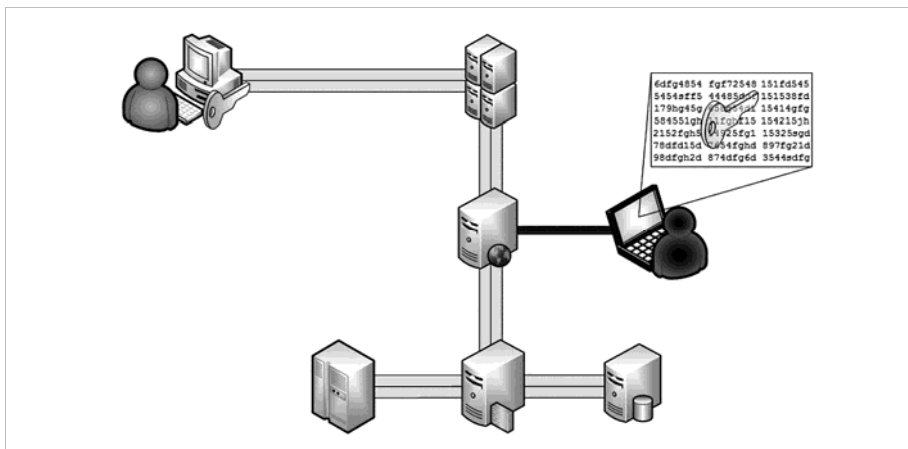


Abbildung 6. Durchgehende Verschlüsselung

2.2 Redundanz

Ein sehr wichtiges Argument für die Nutzung von Cloud-Diensten ist die Möglichkeit der redundanten Haltung von Daten und Diensten. Gerade im medizinischen Bereich ist es wichtig, jederzeit auf notwendige Daten eines Patienten oder einer Behandlung zugreifen zu können oder bestimmte Dienste beispielsweise für die Auswertung von Daten oder deren Speicherung jederzeit zur Verfügung zu wissen.

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.

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. Dies unterscheidet sich von Aktualisierungen, die in der lokalen Infrastruktur eines Krankenhauses vorgenommen werden, wo der Benutzer zumindest kurzzeitig keinen Zugriff auf Programme oder Daten besitzt. 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.

2.3 Lokalisierung von Daten und Diensten

Gerade in Zeiten des Internets stellt man 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. Das TRESOR Projekt setzt beide o. g. Anforderungen von Beginn an um. Darüber hinausgehend ermöglicht der bereits erwähnte modulare Aufbau der Projekt-Infrastruktur aber auch Insellösungen, wenn beispielsweise in bestimmten Ländern restriktivere Anforderungen bezüglich der Datenhaltung bestehen. Dies tritt zum Beispiel im Falle der Schweiz auf, 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]. In diesem Fall ermöglicht TRESOR die Bereitstellung von Diensten und Datenhaltung auf einem entsprechenden IaaS-Anbieter, welcher den Datenschutzanforderungen der Schweizer Gesetzgebung entspricht.

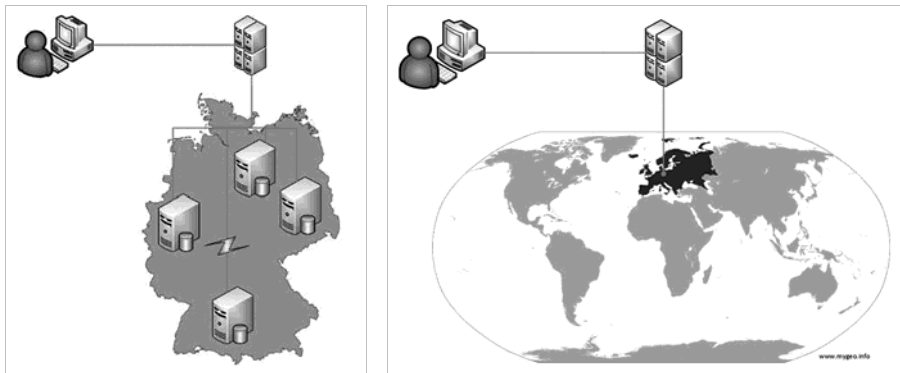


Abbildung 7. Redundante Serverstandorte entsprechend den Anforderungen

3. Anwendungsfälle

Die Umsetzbarkeit der im Rahmen von TRESOR entwickelten Lösungen des Cloud-Ecosystems wird anhand von Anwendungsszenarien aus dem Bereich der Patientenversorgung demonstriert. Ein Projektansatz wird daher die exemplarische

Umsetzung einer medienbruchfreien medizinischen Verlaufsdokumentation sein. Ein weiteres Szenario konzentriert sich auf die Umsetzung eines cloud-basierten, den Behandlungsprozess begleitenden Services zur verlässlichen Prüfung von Arzneimittelinteraktionen auf der Basis aktuellster Informationen.

Die medienbruchfreie medizinische Verlaufsdokumentation (MMV) ist von hoher Bedeutung insbesondere bei der Verlegung von Patienten zwischen Krankenhäusern, in welchen unterschiedliche Krankenhausinformationssysteme verwendet werden und so im Zuge des Sendens von Daten während der Verlegung von einem Krankenhaus in das andere diese Daten für das andere System kompatibel gemacht werden müssen. 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 beispielsweise ein Arzt über den Cloud-Dienst Zugriff auf den medizinischen Verlauf des Patienten im anderen Krankenhaus erhalten, um daraus Schlüsse für eine optimale Weiterführung der Behandlung des Patienten zu ziehen. 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 Datenbank mit Arzneimittel-Interaktionsdaten genommen, um im Zuge der Anordnung einer Medikation zu überprüfen, ob Wechselwirkungen zwischen Medikamenten vorliegen. Der Vorteil eines Cloud-Dienstes liegt hier vor allem in der Möglichkeit des Zugriffs auf tagesaktuelle Daten, die von den Datenbankbetreibern zur Verfügung gestellt wurden und bisher manuell in die bestehende Dateninfrastruktur des Krankenhauses eingepflegt werden mussten.

4. Zusammenfassung

Aufgrund der beteiligten Projektpartner – der medisite Systemhaus GmbH, der T-Systems International GmbH, der bitplaces GmbH, der TU-Berlin und vor allem aber auch dem Deutschen Herzzentrum Berlin und dem Paulinenkrankenhaus Berlin – stellt TRESOR ein interdisziplinäres Kooperationsprojekt dar, in welches das Fachwissen aus unterschiedlichsten Bereichen einfließt und zukünftige Nutzer wie auch Anbieter von Cloud-Diensten eine an gemeinsamen Bedürfnissen ausgerichtete Plattform entwickeln.

Mit TRESOR wird erstmals eine "Trusted Cloud"-Infrastruktur bereitgestellt werden, 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 des Cloud Ecosystems für den Anwendungsbereich der Patientenversorgung wird zukunftsweisend für die weitere Entwicklung von Cloud Enabled Softwareservices im Gesundheitswesen sein.

TRESOR wird gefördert durch das Bundesministerium für Wirtschaft und Technologie aufgrund eines Beschlusses des Deutschen Bundestages.

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 DSGVO CH.
- [7] Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB).
- [8] <http://www.edoeb.admin.ch/datenschutz/00628/00629/00635/index.html> (13.05.2013).