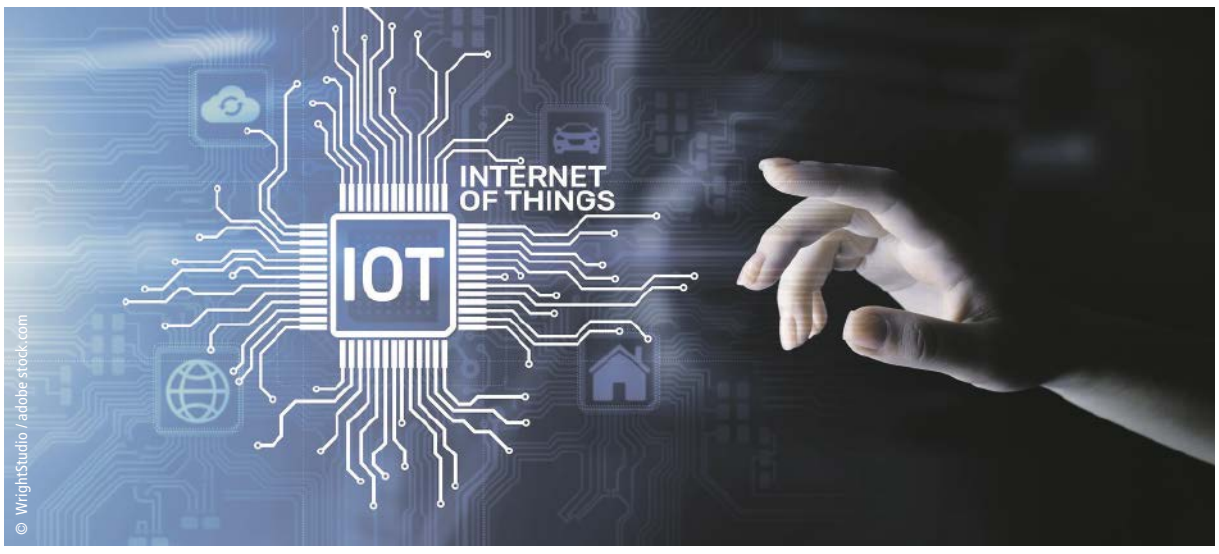

© WrightStudio / adobe stock.com

Internet of Things im vernetzten Krankenhaus

Mit dem Abstraktum „Internet der Dinge" wächst die Bedeutung der Vernetzung von Systemen und Geräten. Für den Datenaustausch sind elementare Protokolle notwendig.

Hans-Otto von Wietersheim, Bretten

Durch Internet of Things (IoT), werden alltägliche Gegenstände mit Informations- und Kommunikationstechnik ausgestattet und somit zu Smart Objects. Immer mehr Dinge werden „smart" mit eingebauten Rechen- und Netzkomponenten. IoT-Geräte haben somit erweiterte Fähigkeiten. Rückgrat des integrierten Gesundheitssystems ist eine auf der Basis moderner Technologien des IoT vernetzte medizinische sowie pflegerische Versorgung von der Wiege bis zur Bahre. Es geht hier um nicht weniger als die fundamentale Digitalisierung unseres Makrokosmos. Gegenstände vernetzen sich zu einem IoT, das im Zusammenspiel mit künstlicher Intelligenz (KI) zu grundlegenden Verwerfungen der bisherigen Lebens- und Arbeitsweise führen kann. Die Vorhersagen für das Zeitalter des IoT erstrecken sich von den verheißungsvollen Arbeitserleichterungen, enormen Effizienzsteigerungen, Wirtschaftswachstum, der Lösung des Fachkräftemangels in einer überalterten Gesellschaft bis zum Defätismus einer apodiktischen Auslöschung ganzer Berufszweige, millionenfachen Arbeitsplatzverlusten, umfassender Überwachung, Beeinträchtigung der sozialen Teilhabe und der existenziellen Frage nach der Entmündigung des Menschen durch Maschinen. Gemeinsamer Nenner dieser teils diametralen Einschätzungen: Das Gesundheitswesen steht wohl vor großen Umwälzungen, wenngleich sich die Bundesrepublik Deutschland nach wie vor der Kritik ausgesetzt sieht, bei der Digitalisierung, insbesondere dem Datennetzausbau, hinterherzuhinken. Außerdem sehen sich Ärzte politischem Druck ausgesetzt, ihre Arztpraxen an die Telematikinfrastruktur anzuschließen und Anwendungen wie die eAU, die ePA oder die sichere KIM zu nutzen. Für die meisten Ärzte erschließen sich die Vorteile der Digitalisierung bisher noch nicht, sie zeigen sich skeptisch bis frustriert. Dies wird in dem im Januar 2022 veröffentlichten „Digitalisierungsreport 2021" deutlich.

IoT-Architektur braucht Sicherheit

Emergente Effekte, bei denen die Gesamtfähigkeiten diejenigen der einzelnen Dinge übersteigen, führen zu einem breiteren Dienstspektrum für die Anwender, bringen jedoch auch neue Herausforderungen mit. Nutzern von IoT-Lösungen im Gesundheitsbereich ist mitunter nicht bewusst, welcher Art von Datenverarbeitung sie zustimmen und welche Daten überhaupt erhoben werden. Die möglichen Bedrohungen und Angriffsvektoren sowie Datenschutzaspekte in IoT-Umgebungen sind nicht immer vollständig offengelegt. Die Herausforderungen hinsichtlich Sicherheit und Datensouveränität werden strukturiert nach verschiedenen Ebenen der Vernetzung als sogenannte Emergenzebenen. Existierende Maßnahmen werden in Fachkreisen diskutiert, wie etwa die Einführung von technischen Richtlinien und Normen oder Zertifizierungsmöglichkeiten. Diese zielen darauf ab, verschiedene Ebenen der IoT-Architektur hinsichtlich Sicherheit und Datenschutz zu verbessern, vernachlässigen jedoch meist die Berücksichtigung von Emergenzeffekten. Dies sollen künftige Lösungsansätze, wie die Einführung von Datensouveränitätsklassen oder Musteranalyse mittels KI, berücksichtigen. Diese Lösungen sind eindeutig durch eine Internetadresse (URL) identifizierbar und über das Internet ansprechbar – aber bei mangelnder Sicherung auch zu kompromittieren. Bislang ungesicherte Lösungen aus dem Bereich des IoT, vor allem Endverbrauchergeräte wie Fitnesstracker und andere Wearables, wurden oft als Angriffsplattform und Einfallstor in Netzwerke und Infrastrukturen missbraucht.

Das sei einerseits darauf zurückzuführen, das Cyber Security noch kein integraler Bestandteil der Produktentwicklung auf Herstellerseite sei, andererseits seien sich aber auch die Anwender der Wichtigkeit von Basis-Sicherheitsmaßnahmen, wie dem Ändern voreingestellter Herstellerpasswörter, noch nicht bewusst. So hätten Angreifer leichtes Spiel. Die Sicherheit der IoT-Devices dürfte nur diffizil zu erreichen sein, weil mit den meist niedrigen Herstellungskosten der Geräte aufwendige Sicherheitsanforderungen verbunden sind.

Anforderungen dominieren IoT

Die Covid-19-Pandemie und die damit einhergehenden Mobilitätsbegrenzungen, Kontaktverbote, Handy-Überwachungs-Apps sowie weitere Strategien zur Eindämmung von Infektionsketten hat im letzten Jahr zu einem eindeutigen Anstieg der Nutzung digitaler Anwendungen im öffentlichen und privaten Gesundheitswesen geführt. Verbesserte Daten-Analysen in der Forschung, Entwicklung und Prüfung von neuen Therapien, sowie das wachsende Potenzial der KI für im Eilverfahren entwickelte diagnostische Methoden und Impfstoffkandidaten, mündete ebenfalls in einer gestiegenen Nachfrage und Anwendung von digitalen Hilfsmitteln unter Ärzten, Patienten, Krankenhäusern, Forschern und Unternehmen. Der Einsatz dieser technischen Innovationen wurde jedoch sowohl von sozioökonomischen und politischen Diskussionen als auch von regen ethischen und rechtlichen Debatten begleitet. Themen wie Datenschutz, Cybersicherheit, Einwilligung, Transparenz, Diskriminierung, Eigentum und eine gerechte Verteilung und Zugang zu den digitalen Möglichkeiten spielen hierbei eine wichtige Rolle. Zutreffend ist diese Thematik auch für KI, KNN, Musterkennung und Robotik, die voneinander abhängen. Wo es um Akzeptanz geht, ist meist auch Transparenz ein großes Thema. Viele Algorithmen ähneln einer Blackbox – selbst für diejenigen, die sie verwenden. Der Grund: Sie werden teilweise extern eingekauft, so dass Entscheidende selbst gar nicht wissen, wie der Algorithmus zu seinem Ergebnis kommt. „Aus wissenschaftlicher und gesellschaftlicher Sicht ist es natürlich wünschenswert zu wissen, wie der Algorithmus einzelne Kriterien gewichtet", so Professor Dr. Frauke Keusch, Universität Mannheim. Auch das sei eine wichtige Voraussetzung für dessen gesellschaftliche Akzeptanz.

Digitale Zwillingstechnologie hilft

Im Zuge der Digitalisierung fast aller Lebensbereiche spielen Digital Twins im Alltagsleben eine immer größere Rolle, vor allem im Rahmen von Anwendungsszenarien wie Smart Home, Connected Car oder im Gesundheitswesen. Digital Twins haben das Potenzial, in vielen Segmenten erheblichen Mehrwert zu schaffen. Sie sorgten für mehr Effizienz, Transparenz und Flexibilität, während sie auf der anderen Seite wirksam Risiken minderten und Qualität sichern könnten. Allerdings bedarf es einer übergreifenden Plattform sowie einer umfassenden Standardisierung von Datenformaten, um das Potenzial digitaler Zwillinge über Insellösungen und geschlossene Plattformen hinaus gänzlich ausschöpfen zu können. Vier Dinge braucht der digitale Zwilling laut einer Studie: Sensoren, Konnektivität, definierte Datenstrukturen sowie ein User Interface, das die relevanten Daten visualisiert. Mit dieser Ausstattung könnten sie im Prinzip überall dort eingesetzt werden, wo vernetzte Objekte vorhanden sind – zum Beispiel in der medizinischen Versorgung. So können z. B. Diabetespatienten ihre Blutzuckerwerte über vernetzte Messgeräte bequem speichern, visualisieren, entsprechend handeln und in Echtzeit an den behandelnden Arzt übertragen. Der Digital Twin erlaubt so das engmaschigere Monitoring der Patienten. Datenaustausch in Echtzeit ist im 5G-Netz möglich So können hochaufgelöste Bilder einer CT quasi verzögerungsfrei an spezielle AR-Brillen übermittelt werden. Ärzte

können die Bilder noch detaillierter auswerten und zielgerichtete Operationen vorbereiten, Patienten noch genauere Diagnosen erhalten und Studierende noch besser auf ihre Arbeit vorbereitet werden.

Technische Merkmale im Detail

Für Vernetzung und Datenaustausch sind Protokolle unentbehrlich. Als wichtigste Protokolle der Application Layer gelten CoAP, XMPP, MQTT, REST, WebSocket, DDS und AMQP. So wurden den wichtigsten Protokollen der Application Layer Anwendungen zugeordnet. Aufgrund der zahlreichen Protokollalternativen sind fehlende Standards in Bezug auf IoT-Infrastrukturen genannt und Standards von Unternehmen gefordert. Das führt gegenwärtig zu einem Forschungsbedarf mit dem Ziel eines Entscheidungsprozesses zur Protokollauswahl. Im Vordergrund stehen die Technologie zur Vernetzung und die Nutzung von Sensordaten. Zum Beispiel wendet CoAP einen User Datagram Protocol (UDP)-basierten Transport an, der zur Folge hat, dass eine Bestätigung des erfolgreichen Transports ausbleibt. Im Gegensatz zu CoAP nutzt MQTT ein Transmission Control Protocol (TCP)-Port, das mehr Zuverlässigkeit bei der Datenübertragung bietet. TCP überprüft hierbei die zu übermittelnden Datenpakete auf Fehlerhaftigkeit und doppelte sowie verloren gegangene Pakete. Neben den Transportmechanismen und den Kommunikationsmodellen ist die Quality of Service (QoS) eine weitere relevante Protokolleigenschaft. QoS ist eine Richtlinie, die verschiedene Attribute für Anwendungsprotokolle beinhaltet. Hierzu zählen Ressourcenauslastung, Datenverfügbarkeit, Datenrechtzeitigkeit und Datenübermittlung. QoS nutzen u. a. CoAP, RESTful HTTP, MQTT, AMQP, DDS. ■