Distributed-Ledger-Technologie

Der digitale Patient muss nicht gläsern sein

31.05.2019 Markus Soppa (Accessec)

Aktuelle Sicherheitsanalysen im Internet der Dinge im Gesundheitswesen zeigen, dass der Schutz von vernetzten Medizingeräten und Patientendaten mangelhaft ist. Vielversprechende Lösungsansätze bieten Distributed-Ledger-Technologien wie Blockchain oder IOTA.

© IOTA

Transparent, aber nicht aus Glas: Durch den gezielten Kryptographie-Einsatz bleibt der Patient auch in Zeiten zunehmender Digitalisierung eigener Herr über seine Daten.

Zweifelsohne ist das Internet der Dinge (Internet of Things, IoT) auch im Gesundheitssektor ein wesentlicher Eckpfeiler neuer wissenschaftlicher Erkenntnisse und die Basis für neue Businessmodelle. Das führt zwangsläufig auch zu Diskussionen, beispielsweise wenn Daten von Fitness-Trackern mit Versicherungsdiensten verknüpft werden. Dieses Geschäftsmodell scheint in greifbare Nähe zu rücken. Doch Sicherheitsexperten wird bei genauerer Betrachtung angst und bange, wenn es um Fragen der Integrität, der sicheren Übertragung und vor allem Datenschutz dieser neuen Dienste geht. Denn Fakt ist: Betreiber von elektronischen Medizingeräten, Dienstanbieter und Infrastrukturbetreiber tun sich schwer, selbst Minimalanforderungen der IT-Sicherheit zu etablieren. Zudem entziehen sich viele Unternehmen, die für den gewünschten Mehrwert enorme Datenmengen benötigen, den regulatorischen Anforderungen, wie zum Beispiel der Allgemeinen Datenschutz-Verordnung der EU (GDPR), gerecht zu werden. Andere ignorieren und verstoßen gegen diese willentlich.

Dem Kunden werden hingegen in erster Linie die Praktikabilität und der Lifestyle der kostenfreien, zum Teil schon auf dem Gerät vorinstallierten Dienste vermittelt. Das Bewusstsein darüber, dass sensible Daten aus der eigenen Hand gegeben werden, führt zum Bild des gläsernen Benutzers beziehungsweise Patienten. Gleichzeitig ist die Verunsicherung der Verbraucher durch die Daten-Sammelwut der Großkonzerne, aber auch durch die vermehrt wahrgenommenen Angriffe durch Hacker auf Daten-Center, Krankenhäuser, Versicherer und Behörden so groß wie nie. So wurden wiederholt Sicherheitslücken in Herzschrittmachern und Insulinpumpen festgestellt.

Immer häufiger geht es zudem um kritische Patientendaten von einigen Medizintechnikherstellern in der Patientenüberwachung. Auch hier ist der Schutz vor Cyberangriffen und unbefugten Zugriff im Gerät und in der IT-Zielinfrastruktur immer noch keine Selbstverständlichkeit – trotz der kontinuierlich steigenden

Bedrohungslage. Dass medizinische Geräte zunehmend mit Mobiltelefonen, Tablet-Computern oder anderen tragbaren Geräten und Cloud-Diensten verschmelzen, stellt ein zusätzliches erhebliches Sicherheitsrisiko dar. Denn nicht nur die Daten, sondern auch die Kontrolle über die Geräte könnte hierdurch in falsche Hände geraten.

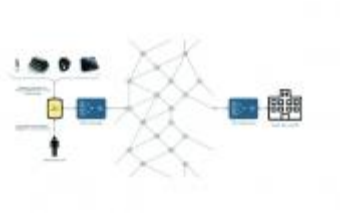
Die Konvergenz von Netzwerken, Computertechnologien und Software sowie die zunehmende Integration von Krankenhaus-Enterprise-Systemen, Informationstechnologie und klinischem Engineering und Lieferanten verstärken bereits heute die wahrnehmbaren Risiken. Anwendungsfälle wie Remote-Konnektivität oder Data Analytics bieten eine weitere Angriffsfläche. Zwar sind viele dieser Risiken nach heutigem Stand lösbar, jedoch kommen, wenn überhaupt, nur in Medizingeräten Zertifikate und Public Key-Infrastrukturen zum Schutz der Geräte zum Einsatz.

Sprechen wir hingegen von dem hochvernetzten und verfügbaren IoT, stoßen diese bewährten Lösungen an ihre technischen Grenzen. Für eine hochvernetzte und optimierte Medizinversorgung bedarf es dringend vertrauenswürdiger Technologien. Diese sollten sich auch auf Kleinstgeräten unterbringen lassen, kostengünstig sein und im besten Falle dem Kunden beziehungsweise Patienten die Hoheit seiner sensiblen Daten überlassen. Ein vielversprechender Ansatz ist die Distributed-Ledger-Technologie, wie das kostenfreie Protokoll der IOTA-Foundation (abgeleitet vom kleinsten Buchstaben im griechischen Alphbet Iota).

Eigenart und Brauchbarkeit des IOTA-Tangles

Blockchain mit Bitcoin oder Ethereum sind sicherlich die bekanntesten Beispiele für die Distributed-Ledger-Technologie (DLT). Mit der dritten Generation ist die DLT jedoch von ihrer ursprünglichen Form weit entfernt. So wurde IOTA unter anderem für sichere IoT-Anwendungen entwickelt und gilt mittlerweile als gewinnversprechende Variante von Blockchain. Dabei handelt es sich im engeren Sinne gar nicht um eine Blockchain, sondern um einen Directed Acyclic Graph (DAG) [1], der die positiven Eigenschaften der Blockchain vereint. Die »Winternitz hash«-basierte Verschlüsselung ist zudem nicht nur schneller als die »Elliptic Curve«-Kryptographie, sondern verspricht auch Quantencomputer-Resistenz. Darüber hinaus ist der DAG partitionstolerant, schnell und kommt im Gegensatz zur klassischen Blockchain oder anderen Distributed-Ledger-Technologien komplett ohne Transaktionsgebühren und Miner aus. Das Datenschema ist zudem so gewählt, dass der Tangle-Ansatz faktisch unbegrenzt skalieren kann [2].

Mit diesen Eigenschaften bildet der Tangle die ideale Grundlage für anknüpfende Technologien im IoT, etwa bei technologisch limitierten medizinischen Geräten. Das Protokoll punktet nicht nur durch seine Interoperabilität, sondern ermöglicht IoT-Teilnehmern unterschiedlicher Art, sicher miteinander mittels sogenannter Datentransaktionen zu kommunizieren, ohne die Sicherheit zu gefährden. Dieser entscheidende Vorteil könnte IOTA langfristig zu einer echten Option für diejenigen machen, die die Digitalisierung im eigenen Unternehmen beziehungsweise Institut mit Zukunftstechnologien vorantreiben wollen – immerhin lassen sich Transaktionen oder Daten direkt auf dem DAG speichern. Tatsächlich ist der Tangle einer der wenigen verfügbaren Distributed-Ledger-Technologien, die bisweilen nicht gehackt werden konnten und befindet sich als bislang einziges DLT-Protokoll in der Standardisierung.



© IOTA

Im Gegensatz zur Bitcoin nutzt IOTA keine Blockchain, sondern einen gerichteten azyklischen Graphen (englisch: Directed Acyclic Graph, DAG).

Teil 1 von 2

1. Der digitale Patient muss nicht gläsern sein
2. Anwendungsfälle in der Medizin