Weniger ist mehr – Reduktion und Abstraktion von Daten in der vernetzten Welt

Kerbusch, Jochen; Kempa, Heiko; Heinrich, Anett; Spitzner, Eike-Christian
VDI/VDE Innovation + Technik GmbH, Berlin / Dresden

Kurzfassung

Die zunehmende Digitalisierung nahezu aller Lebensbereiche erfordert die vernetzte Bereitstellung enormer Datenmengen. In diesem Zusammenhang nehmen die Anzahl lokal genutzter Sensoren und das zu übertragende Datenvolumen drastisch zu. Dabei spielen Themen wie die Sicherheit im Sinne der Integrität sowie der Verfügbarkeit der erfassten Daten eine entscheidende Rolle zur Gewährleistung der gewünschten Funktionalität in der geforderten Qualität. Ein oft unterschätzter, aber wesentlicher Teil dieser Entwicklung ist eine leistungsfähige und effiziente Datenvorverarbeitung. Häufig ist die Übertragung lokaler Sensorrohdaten an Steuerrechner bzw. „Big Data“-Infrastrukturen wenig sinnvoll. Vielmehr ist eine Reduktion der Daten auf die für die weitere Verarbeitung wesentliche Information bereits am Ort der Messung vorteilhaft. Dies schont Übertragungskapazitäten, ermöglicht die Aussortierung nicht valider Daten, die Anonymisierung der Daten bereits am Punkt der Aufnahme und birgt enorme Effizienzpotenziale. Entsprechende Lösungen sind sowohl in Soft- als auch in Hardware umsetzbar. Beides bietet komplementäre Vor- und Nachteile.

1. Motivation und Vision

Die Digitalisierung hält nicht nur in Wirtschaft und Gesellschaft, sondern in unser tägliches Leben Einzug. Schlagworte wie Internet der Dinge, Industrie 4.0 oder Smart Home sind in aller Munde. Der Schlüssel zu Innovationen in diesen Bereichen liegt heutzutage nahezu ausschließlich in der Vernetzung intelligenter Geräte und der damit möglichen Nutzung vieler, dezentral gewonnener Daten. Die Vision ist das umfassende Sammeln aller verfügbaren Messdaten, um sie mit Hilfe von „Big Data“-Ansätzen auszuwerten und auf dieser Basis neue Dienstleistungen anzubieten.

Dabei ist neben der Quantität vor allem die Qualität der genutzten Informationen entscheidend für die Brauchbarkeit der darauf basierenden Anwendungen. Ein wesentlicher Beitrag hierzu ist eine leistungsfähige und effiziente Datenvorverarbeitung. Statt riesige Mengen unbearbeiteter Rohdaten von lokalen Messstellen an eine übergeordnete Infrastruktur (z.B. Cloud-Dienste) zu schicken, ist es oft sinnvoller, den Datenstrom mit Hilfe effizienter Hardware bereits am Ort der Messung unter Berücksichtigung von Datensicherheit und Datenschutz auf die für die Verarbeitung wesentlichen Informationen zu reduzieren.

Bereits heute sind wir im privaten wie auch beruflichen Alltag von einer Vielzahl von Sensoren und Datenknoten umgeben: Schlafüberwachung durch das Smartphone, Sprachsteuerung für Licht und Haushaltsgeräte, Fitnesstracker, Fahrerassistenzsysteme im Auto, RFID-basierte Schließsysteme, autonome Flurförderfahrzeuge, Zustandsüberwachung in der Produktion, um nur einige wenige Anwendungsfelder zu nennen. Wir leben bereits heute in der vernetzten Welt von morgen.

Bei den genannten Beispielen handelt es sich zumeist um Sensor- und Elektroniksysteme, die jeweils auf Basis relativ weniger Messdaten, vereinzelt auch online, kommunizieren, aber letztendlich lokal begrenzt agieren. In Summe sind die gewonnenen Informationen jedoch vielfältig und ermöglichen zusammengeführt noch deutlich höherwertige Dienstleistungen als jeweils für sich genommen. Doch was bedeutet es technisch, wenn wirklich alle Sensoren alle Messdaten permanent über Datennetze an eine oder mehrere externe Stellen senden, wie in Abb. 1 gezeigt?

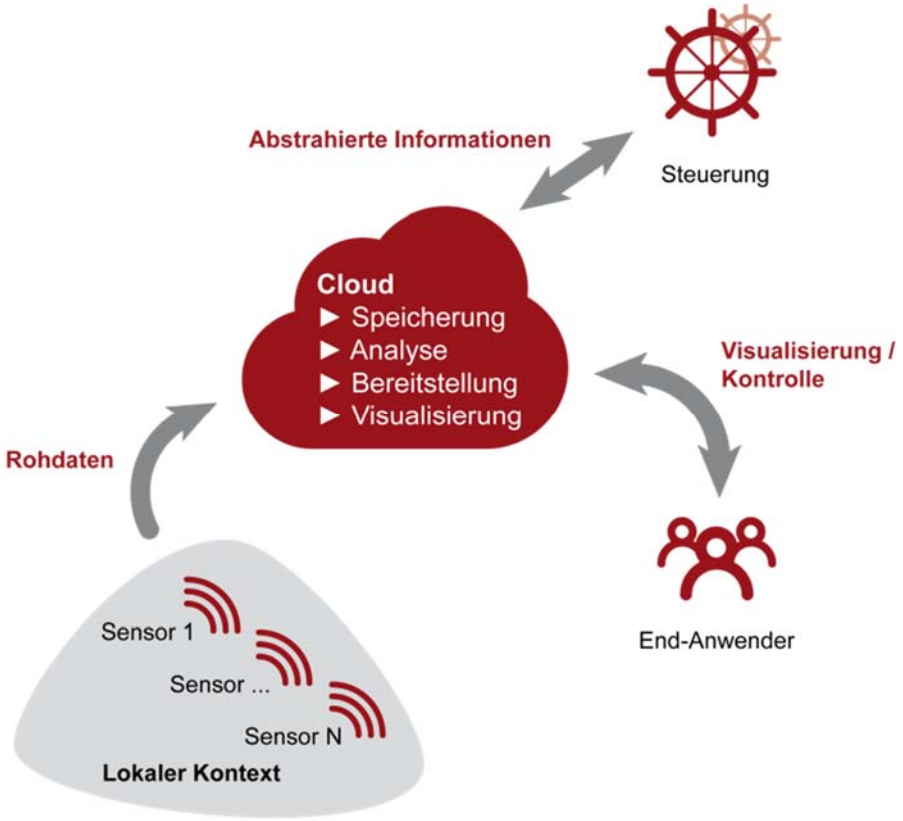

Abb. 1: Übliches Konzept der Cloud-basierten Dienste: Lokale Sensoren kommunizieren alle Rohdaten zur Auswertung und Bereitstellung an die Cloud, auf die Endanwender sowie Steuerinstanzen zugreifen können.

Heute greifen etwa 15 Milliarden Geräte auf das Internet zu. Durch das Internet der Dinge wird diese Zahl zweifelsfrei stark anwachsen. Manche Experten gehen von bis zu 50 Milliarden weltweit vernetzten Geräten im Jahr 2020 aus [1], andere von 500 Milliarden im Jahr 2030 [2]. Smarte Systeme sind in der Regel permanent in Betrieb.

Dauerhaft große Datenmengen durch das Internet zu senden ist jedoch schon aus technischer Sicht keine Lösung.

Geht man von 500 Mrd. Geräten aus, so würde bereits das Verschicken je eines Bytes an Information pro Sekunde enorme Übertragungskapazitäten im Bereich von einem halben Petabit/s voraussetzen. Dabei ist dies nur eine Minimalbetrachtung: Zum einen lassen sich mit einem Byte pro Sekunde kaum relevante Messdaten übertragen, zum anderen sind das Protokoll oder gar Kommunikation mit mehreren Knoten nicht berücksichtigt. Sendet eine größere Menge von vernetzten Sensorsystemen unverarbeitete Rohdaten, im Extremfall hochaufgelöste Videodaten, so wird der Ansatz, alle Daten ohne Vorverarbeitung zu senden, allein aus Gründen der Übertragungskapazitäten technisch schnell unmöglich.

Darüber hinaus stellen sich wichtige Fragen bezüglich der Sicherheit der zu übertragenden Daten, sowohl im Hinblick auf den Missbrauch durch externe Stellen als auch auf die Interessen der Nutzer, sei es Wahrung der Privatsphäre oder auch wirtschaftliche Interessen an den Daten (Datensouveränität). Im Kontext der Datenvorverarbeitung fällt diesen Punkten ebenfalls eine zentrale Bedeutung zu.

Wie schnell sich das Internet der Dinge zu einer Gefahr für die Infrastruktur wandeln kann, wurde Ende September 2016 sichtbar, als drei Jugendliche aus Alaska erstmalig das sogenannte Mirai-Botnet einsetzten, um konkurrierende Minecraft-Server auszuschalten [3]. Rund zwei Monate später wurde die gleiche Technik für einen großangelegten Angriff auf DSL-Router der Telekom eingesetzt. Möglich wurden diese Angriffe durch Sicherheitslücken in vernetzten Geräten, die entweder nicht geschlossen werden können oder die durch die Hersteller nicht gesichert werden. Beide Vorfälle führten zu erheblichen Ausfällen in den Datenverbindungen nicht nur der eigentlichen Ziele, sondern auch zahlreicher anderer Einrichtungen. Im Zeitalter der digitalen Geschäftsmodelle kann ein derartiger Ausfall ein Unternehmen an den Rand des Ruins und darüber hinaus sowie weitergehende Konsequenzen mit sich bringen. Ein umfassendes Sicherheitskonzept muss also zentraler Bestandteil jeder Produktentwicklung von vernetzten Geräten sein.

2. Reduktion und Abstraktion von Daten

Um die wachsende, aber immer begrenzte Bandbreite nicht zu sprengen, sind Konzepte erforderlich, die die Datenflut eindämmen. Dies kann durch Auslassen von Messwerten geschehen. Nicht für alle Anwendungen sind Echtzeitdaten erforderlich, sondern weitaus längere Messintervalle ausreichend. Doch das ist nur ein Anfang. Ein Sensor, der periodisch einen Messwert zur Zustandsüberwachung ausgibt, produziert und kommuniziert Unmengen an irrelevanten Daten über den Normzustand. Stattdessen kann ein regelmäßiges Lebenszeichen und gegebenenfalls ein Fehlersignal gesendet werden. Üblicherweise sind erst dann weitere Informationen erforderlich, die

bedarfsgerecht abgerufen werden können. Ein weiteres Beispiel sind bildverarbeitende Systeme, wie sie zur Objektverfolgung in Fahrerassistenzsystemen häufig eingesetzt werden. Anstelle von räumlich wie zeitlich hochaufgelösten Vollbildern können reine Objektinformationen ausgegeben und damit nur die relevanten Informationen weiter geleitet werden.

Einer der wichtigsten Aspekte in der Datenvorverarbeitung ist die Echtzeitfähigkeit der Datenreduktion, die nur durch eine hohe Rechenleistung erzielt werden kann. Diese wiederum erfordert entweder einen hohen Energieeinsatz (Mikrocontroller) oder eine starke Spezialisierung auf Hardwareebene (ASIC). Ersteres führt zu verkürzten (Akku-)Laufzeiten, letzteres zu einem Verlust an Flexibilität und zunächst erhöhten Kosten. Weiterhin können an eine spezielle Aufgabe angepasste Verarbeitungssysteme nicht auf einfache Weise während der Lebensdauer modifiziert werden. Ihre Funktionen und ihre Datenausgabe werden zum Zeitpunkt der Entwicklung vorgegeben. Dem gegenüber steht eine erheblich höhere Leistungsfähigkeit der spezialisierten Funktionen bei gleichzeitig geringerem Energieverbrauch gegenüber auf Mikrocontrollern ausgeführten, softwarebasierten Systemen. Gerade im Bereich der Sensornetzwerke ist dies ein sehr wichtiger Aspekt, da einzelnen batteriegespeisten Knoten nur geringe Energiemengen zur Verfügung stehen. Es muss also aus technologischer Sicht ein Kompromiss aus Leistungsfähigkeit, Energieeffizienz und Flexibilität gefunden werden. Dabei dürfen die Aspekte der Datensouveränität jedoch ebenfalls nicht außer Acht gelassen werden.

3. Datenvorverarbeitung als modularer Baukasten

Da das Anwendungsspektrum zu breit ist, um einen allgemeingültigen Kompromiss zu formulieren, muss jeweils das anwendungsspezifische Optimum gefunden werden. Dabei würde ein modularer Baukasten aus Hardwarekomponenten für spezifische, besonders zeit- und energiekritische Aufgaben und Softwaremodulen für den flexiblen Einsatz maßgeschneiderte Lösungen ermöglichen. Es existieren zahlreiche mathematische und informationstechnische Verfahren, die auf den jeweiligen Anwendungsfall zugeschnittenen zum Einsatz kommen und hauptsächlich die Aufgaben der Bereinigung und Reduktion von Daten sowie der Extraktion von Informationen erfüllen. Die zugrunde liegenden Algorithmen können sowohl als Software, als auch als Hardware in Form von diskreten oder integrierten mikroelektronischen Schaltungen umgesetzt werden.

Aufgrund der enormen Geschwindigkeit moderner Prozessoren und ihres ohnehin großen Energieverbrauchs fällt der erhöhte Bedarf an Rechenzeit und Energie einer Softwareimplementierung nur noch selten ins Gewicht. Deshalb wird die Datenvorverarbeitung bei herkömmlichen Anwendungen meist in derselben Hardwareumgebung wie

die eigentliche Datenauswertung ausgeführt und typischerweise als Software implementiert. Dadurch werden Hardwarekosten eingespart und Flexibilität bei der Programmierung gewonnen. Auf der anderen Seite müssen alle Rohdaten übermittelt werden, was die Bandbreite belastet, Sicherheitsfragen aufwirft und ein hohes Maß an Energie kostet.

Für autonome Sensorsysteme oder Mobilgeräte mit ihrem stark begrenzten Energiebudget und hohen Anforderungen an die Rechenleistung ist die Abwägung der Implementierungsoptionen erneut von Relevanz. Dies gilt insbesondere für die Vorverarbeitung der Sensordaten, die von der zentralen Hardware in die einzelnen Sensorknoten verlagert wird, in erster Linie aufgrund der endlichen Bandbreite.

Hinzu kommt, dass die Möglichkeiten zur Implementierung der Datenvorverarbeitung in Sensorsystemen aufgrund der zunehmenden Funktionsintegration in der Mikroelektronik erweitert werden. Durch die gemeinsame Verarbeitung von digitalen und analogen Signalen in sogenannten Mixed-Signal-Schaltungen und durch die Integration logischer Funktionalitäten mit leistungselektronischen Komponenten können Bauraum und Energieverbrauch verringert werden.

Die oben genannten Schritte in der Datenvorverarbeitung stützen sich zumeist auf immer wiederkehrende Algorithmen, z.B. analoge oder digitale Filter oder gleitende Durchschnittsbildung für die Rauschunterdrückung, Fourier- und Laplace-Transformationen, Kantendetektion oder Kreuzkorrelationen sowie Verschlüsselung. Diese können zu einer umfassenden Bibliothek an hochoptimierten Komponenten – diskret aufgebaut oder als IP-Core – mit einheitlichen Schnittstellen zusammengefasst werden. Wird dabei jede Komponente sowohl als Hardware- als auch als Software-Baustein angelegt, lässt sich auf einfache Weise eine heterogene Datenverarbeitungskette auf den spezifischen Anwendungsfall maßschneidern, so dass die Anforderungen an die Leistungsfähigkeit, Flexibilität, Sicherheit sowie Energie- und Kosteneffizienz bestmöglich erfüllt werden. Abb. 2 veranschaulicht das Konzept.

Aus Sicht der Systemanbieter müssen Systeme zur Datenreduktion und Abstraktion neben der Möglichkeit des Maßschneiderns anwendungsspezifischer Lösungen einfach in der Handhabung und Integration sein. Dies kann nur durch ein hohes Maß an Selbstorganisation und Selbstkonfiguration erreicht werden. Jedoch bergen solche automatisierten Routinen sicherheitsrelevante Risiken in sich.

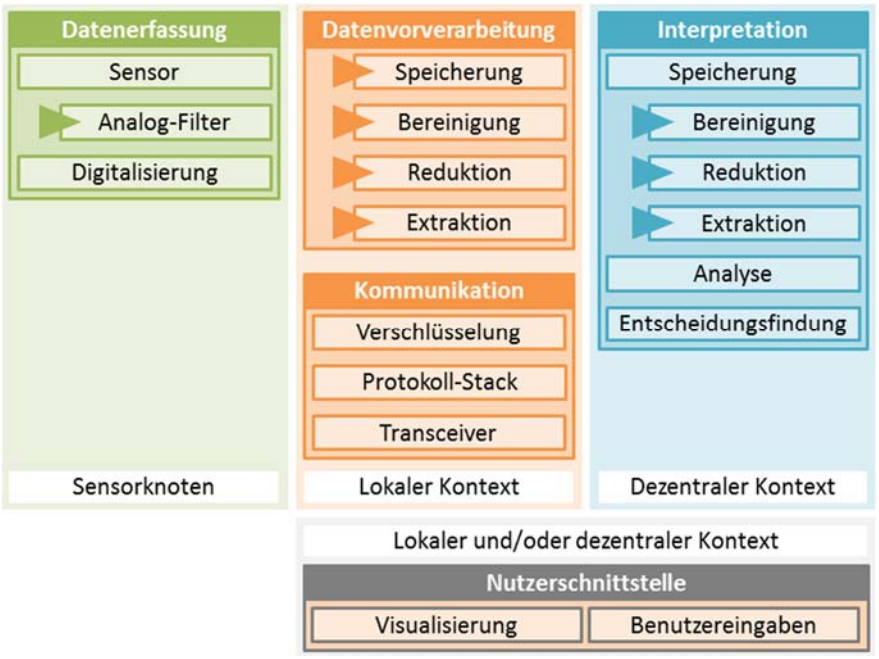

Abb. 2: Blockschaltbild eines modular aufgebauten Datenerfassungssystems vom Sensorknoten über die Datenvorverarbeitung bis zum Cloud-Dienst. Optionale Module sind mit einem Dreieck gekennzeichnet.

Aus Sicht der Endanwender stehen vor allem die großen wirtschaftlichen Chancen im Vordergrund, die durch allumfassende Vernetzung und darauf basierenden Geschäftsmodellen entstehen. Wichtig ist dennoch, dass die Datenflut schon am Ort der Messung gefiltert wird, denn Daten an sich schaffen keinen Wettbewerbsvorteil, dieser hängt vielmehr wesentlich von der Auswertung ab. Beispielsweise kann die Vernetzung von Geräten und Prozessen im Gesundheitswesen die Effizienz von Behandlungen und der Pflege steigern. So lassen sich Gesundheitsdaten von Patienten unabhängig vom Aufenthaltsort automatisiert erfassen und auswerten. Diese Vernetzung birgt neben enormen wirtschaftlichen Chancen für Unternehmen auch erhebliche Risiken der Verletzung der Privatsphäre und des Informationsmissbrauchs.

Das Zusammenführen von Daten ohne Legitimation und Kontrolle birgt inhärent das Potenzial einer informationellen Ausbeutung und kann die Grundrechte der Menschen massiv verletzen. Der Zugriff auf persönliche Daten und deren Monetarisierung durch Weitergabe an Dritte führt zudem zu einer nicht unerheblichen Änderung der Geschäftsbeziehung. Dass der Nutzer in einem solchen Fall anstatt mit Geld durch Preisgabe seiner Daten bezahlt, greift deutlich zu kurz. Vielmehr verliert er die Rolle des Kunden. Diese wird stattdessen vom Endabnehmer der Daten eingenommen, z.B. einem Werbetreibenden. Der Dienstanbieter wird im Sinne seiner Kunden agieren, was deutlich von den Interessen der Nutzer abweichen kann. Deshalb spielen umfassende Sicherheitskonzepte in der vernetzten Welt eine zentrale Rolle. Alle Systeme, die über das Internet miteinander verbunden sind, können kompromittiert und die übermittelten

Daten missbraucht werden. Es gilt der Grundsatz: „Alles was gehackt werden kann, wird auch gehackt!“ (Zitat Sabine Herlitschka, Vorstandsvorsitzende Infineon Austria, in [4]). Somit ist jedes mit dem Internet verbundene Gerät grundsätzlich in Gefahr.

Um ausreichende Sicherheitskonzepte zu etablieren, müssen Unternehmen zunächst investieren. Ein Lösungsansatz besteht in einer effektiven und effizienten, Hardware-basierten Datenvorverarbeitung auf Sensorebene oder hierarchisch gestaffelt auch auf Ebene eines oder mehrerer Gateways, die die Daten aus vielen Sensoren zu einer Gesamtinformation verschmelzen und abstrahieren, wie es mit dem „Fog Computing“ vorgeschlagen wurde (siehe weiter unten sowie [5]).

Die Implementierung entsprechender Infrastrukturen muss bereits in der Planungsphase mit einbezogen werden, da nachträgliche Umsetzungsversuche meist zum Scheitern verurteilt sind. Wichtige in Betracht zu ziehende Aspekte sind die Weiterleitung und Speicherung von lediglich notwendigen Daten, deren Verschlüsselung sowie ein separater Schutz der gespeicherten Daten auf dem Server. Angriffe auf die Sicherheit lassen sich grundsätzlich nicht ausschließen. Daher gilt es, den Angreifern so wenig Angriffsfläche wie möglich zu bieten. Vorteil der hardwarebasierten, sensornahen Datenvorverarbeitung ist die selektive Weitergabe von Informationen. Nur hardwarebasiert kann eine definitive Filterung realisiert werden. Dies führt zu einer Reduktion der zu übertragenden Daten und damit auch zu erhöhter Sicherheit.

Umfassendes Risikomanagement, wie in der ISO 27001 gefordert, ist also ein weiterer wichtiger Aspekt für erfolgreiche Systeme zur Datenreduktion und Abstraktion. Ein hoher Grad an Verschlüsselung sowie der inhärent erhöhte Schutz der Privatsphäre durch die Abstraktion von Daten am frühestmöglichen Punkt im System bilden dafür die Grundlage. Verfügbarkeit und Integrität sind für das einwandfreie Funktionieren Cloud-basierter Anwendungen erforderlich. Hier ist im Einzelfall abzuwägen, wie kritisch die Verfügbarkeit der auf den Daten basierenden Anwendung ist. Im gleichen Zuge bestehen hohe Anforderungen an die Datenqualität. Die Abstraktion wird per se die Qualität erhöhen, jedoch müssen die anwendungsspezifischen Systeme eine entsprechend hohe Erkennungsrate aufweisen. Insbesondere bei der Überwachung kritischer Funktionen dürfen wichtige Ereignisse nicht „übersehen“ werden. Fehlalarme sind zwar ebenfalls unerwünscht, jedoch durch eine Überprüfung als solche erkennbar und deshalb als weitaus weniger kritisch einzustufen.

Ein Ansatz, der zunehmend auf positive Resonanz stößt, ist das sogenannte „Fog Computing“ [5]. Es basiert auf lokalen Gateways, die zwischen externen Cloud-Systemen und die lokalen Knoten geschaltet werden, gegebenenfalls in mehreren Hierarchieebenen (siehe Abb. 3). Die Gateways können beispielsweise auf der Ebene einzelner Räumlichkeiten, Gebäude oder sogar Maschinen angesiedelt werden. Jedes Gateway verarbeitet die Informationen einer definierten Anzahl von Sensor- und Datenknoten, d.h. Rohdaten oder abstrahierte Daten, und liefert eine Schnittstelle an

übergeordnete Strukturen sowie Auswerteknoten oder Bedieneroberflächen. Die Weiterleitung relevanter, abstrahierter Informationen erfolgt dann innerhalb der Hierarchieebene oder an die übergeordnete Struktur.

Dieses Konzept bietet eine Reihe von Vorteilen gegenüber einer permanenten, vollständigen Anbindung an die Cloud. Zunächst besteht aufgrund der schnelleren lokalen Netzwerkverbindung ein höherer Datendurchsatz, so dass zeitkritische Aufgaben schneller koordiniert werden können. Das über das Internet an die Cloud zu übertragende Datenvolumen wird deutlich reduziert, so dass auch hier Leistungsvorteile entstehen. Die Daten können außerdem im lokalen Kontext besser geschützt werden, da sie ihn nicht oder nur in abstrahierter Form verlassen.

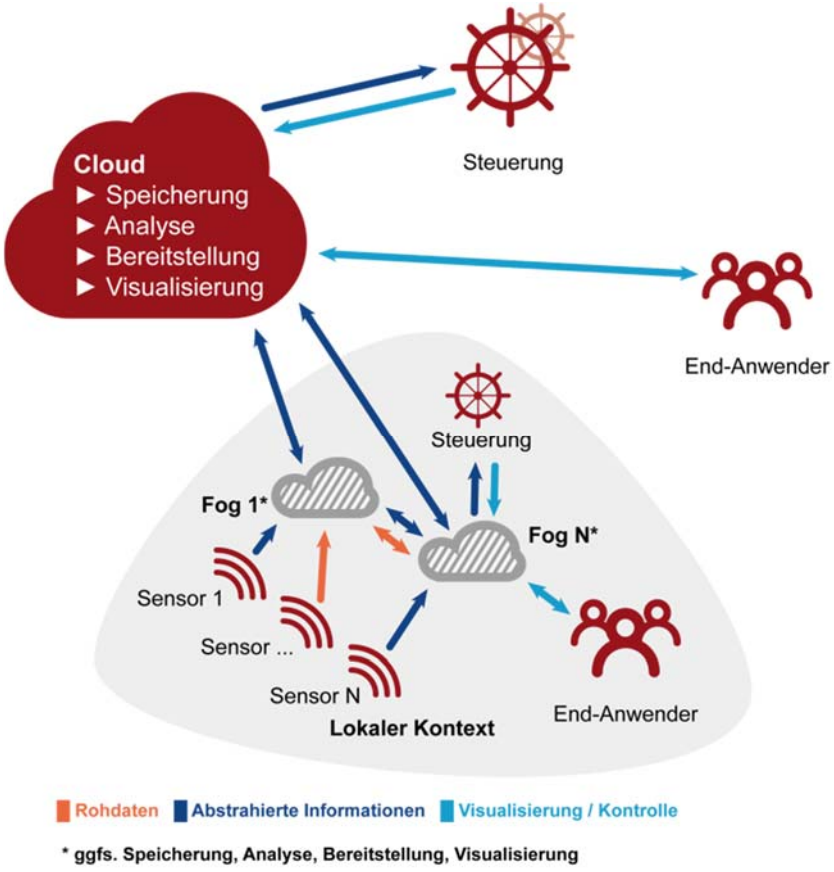

Abb. 3: Konzept des „Fog Computings“: Lokale Sensoren kommunizieren abstrahierte und/oder Rohdaten an einen lokalen Verbund („Fog“), der wiederum nur abstrahierte Daten an die Cloud weiterleitet oder von dort erhält bzw. den Zugriff im lokalen Kontext erlaubt. Über die Cloud können externe Endanwender sowie Steuerinstanzen nur indirekt auf die Sensordaten zugreifen.

Zahlreiche digitale und vernetzte Anwendungen sind bereits Realität. Es existieren in der Praxis Unmengen an Kommunikationsprotokollen. Auf Seiten der Algorithmen zur Datenverarbeitung ist die Auswahl ebenfalls groß, die mathematischen Grundlagen sind teilweise seit Jahrzehnten bekannt. Die Umsetzung in hocheffiziente Software-

Produkte oder Hardware-Komponenten stellt ebenfalls eine untergeordnete Herausforderung dar. Welche technologischen Innovationen fehlen also?

Die Antwort ist prägnant: Keine! Alle erforderlichen Einzelbausteine auf Seiten der Software oder Hardware sind im Wesentlichen vorhanden. Es mangelt in erster Linie an einer Vereinheitlichung, d.h. einer Fusion der Protokolle, Schnittstellen und Einzelkomponenten zu einem strukturierten, flexiblen und offenen Standard. Erst dadurch wird eine durchgängige Kette mit „Security by Design“-Ansätzen möglich. Diese sind derzeit nicht verfügbar bzw. werden nur unzureichend umgesetzt, wie zahlreiche Meldungen über Sicherheitslücken in vernetzten Geräten beweisen [3].

4. Fazit

Der Bedarf einer effizienten Reduktion und Abstraktion von Daten ist evident. Weiterhin sind auf den individuellen Anwendungsfall maßgeschneiderte Lösungen unerlässlich. In vielen Fällen ist dabei ein hardwarebasierter Ansatz aufgrund der besseren Sicherheit sowie der höheren Effizienz einer reinen Softwarelösung vorzuziehen. Die technischen Voraussetzungen dafür sind im Wesentlichen bereits heute erfüllt. Die größten Hürden bestehen im Fehlen einer Standardisierung, einem Mangel an modularen, kompatiblen Konzepten und in der Tatsache, dass eine flexible Standardtechnologie ausgewählt werden müsste, auf der anschließend kontinuierlich weiter aufgebaut wird, anstatt immer neue Technologien aufzusetzen. Darüber hinaus ist der Ansatz, den Idealzustand in der Verschmelzung und Analyse aller theoretisch verfügbaren Informationen zu sehen, kritisch zu hinterfragen.

Erst mit Einzug der genannten Faktoren in die Umsetzung von vernetzten, digitalen Dienstleistungen kann eine für alle Seiten vorteilhafte Wertschöpfung erfolgen. Für kleine und mittelständische Unternehmen sind hardwarebasierte Lösungen, die speziell auf ihre Anwendungsgebiete ausgerichtet, zugleich stromsparend und angriffsgeschützt sind, eine nicht unerhebliche Investition. Um auch diese Unternehmen von hardwarebasierten Lösungen zur Datenvorverarbeitung überzeugen zu können, ist es notwendig, standardisierte Einzelpakete dieser Hardware als einen individuell erweiterbaren Baukasten zu entwickeln und diesen dann in der Massenproduktion kostengünstig anzubieten. Erst damit können neue Geschäftsmodelle aufgebaut und bestehende der Zeit angepasst werden. Die Anbieter solcher Systeme profitieren von einem Standard durch neue Produkte. Nicht zuletzt profitieren die Anwender von einfacher, sicherer Handhabung und von der Gewissheit, dass ein Informationsmissbrauch erschwert wird. Datensicherheit kann, ebenso wie Energieeffizienz und Benutzerfreundlichkeit, in einer Welt im Wandel niemals ein Zustand sein, sondern wird immer ein Prozess bleiben.

Literatur

[1] Hein, Mathias: Kommentar: Internet der Dinge. Risiken des IoT, funkschau, 05.03.2015. www.funkschau.de/datacenter/artikel/117680, 18.07.2016.

[2] Bundesministerium für Wirtschaft und Energie (BMWi): Impulse für die Digitalisierung der deutschen Wirtschaft. Digitale Agenda des BMWi. http://www.bmwi.de/DE/Mediathek/publikationen,did=727322.html, 18.07.2016.

[3] Wikipedia-Artikel „Mirai (Malware)“. https://de.wikipedia.org/wiki/Mirai_(Malware), 04.02.2018.

[4] Dobrowolski, Piotr: Interview: „Pflegeroboter sind eine attraktive Idee“. Wiener Zeitung, 12.12.2015. http://www.wienerzeitung.at/themen_channel/wz_reflexionen/zeitgenossen/790661_Pflegeroboter-sind-eine-attraktive-Idee.html, 23.08.2016.

[5] http://fognetworks.org/whitepapers, 18.07.2016.

Kontakt

Dr. Jochen Kerbusch
VDI/VDE Innovation + Technik GmbH
Kramergasse 2
01067 Dresden
E-Mail: jochen.kerbusch@vdivde-it.de