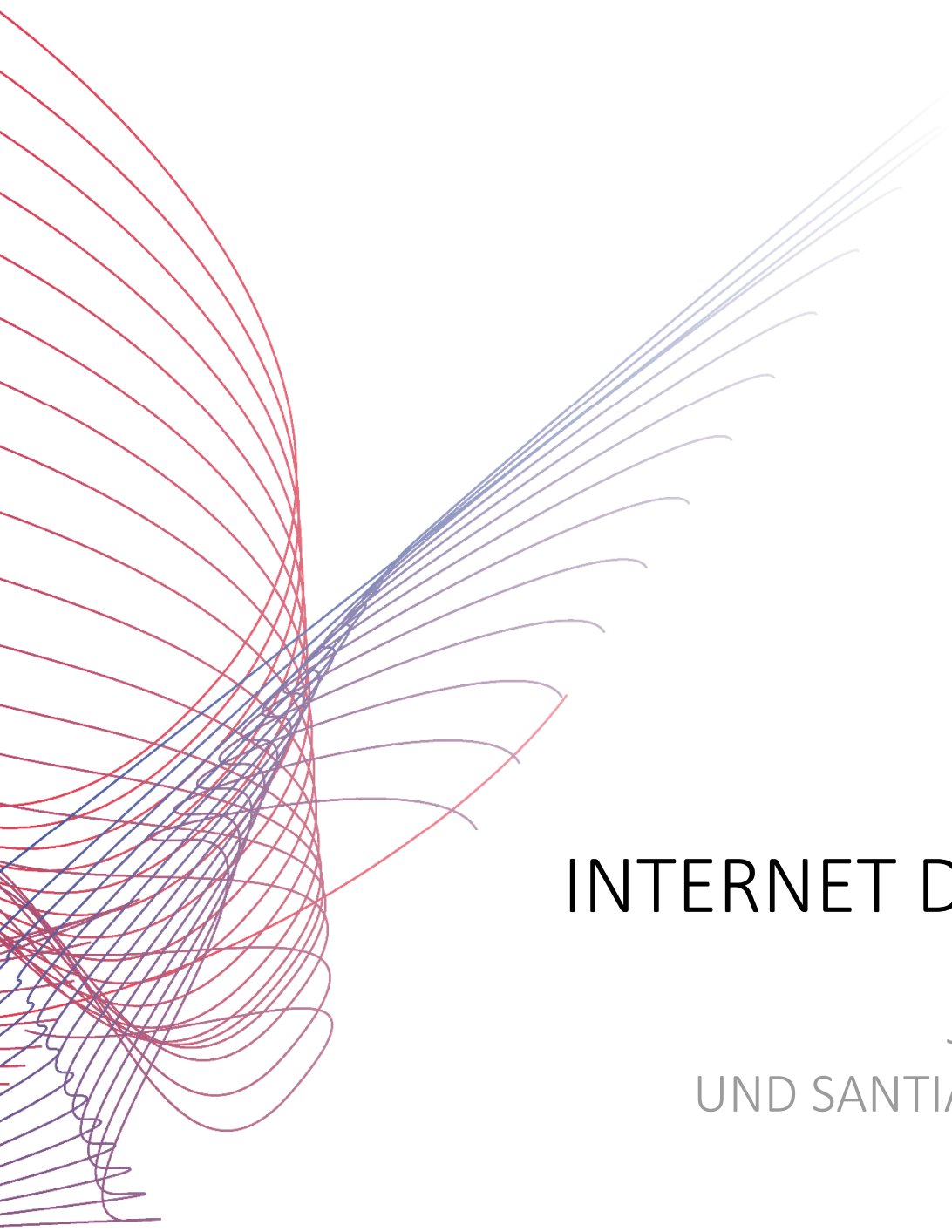
en cs de sk es

TECH pedia



INTERNET DER DINGE

JORDI SALAZAR
UND SANTIAGO SILVESTRE

Titel der Arbeit: Internet der Dinge
Author: Jordi Salazar und Santiago Silvestre
Übersetzt (von): Radoslav Vargic
Veröffentlicht (von): České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktadresse: Technicka 2, Prague 6, Czech Republic
Tel.: +420 224352084
Drucken: (nur elektronisch)
Anzahl der Seiten: 34
Ausgabe: 1. Ausgabe, 2017

ISBN 978-80-01-06233-3

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ERLÄUTERUNG

	Definition(en)
	Interessantheit (Interessantes)
	Bemerkung
	Beispiel
	Zusammenfassung
	Vorteile
	Nachteile

ZUSAMMENFASSUNG

Dieser Kurs bietet die Einführung zum Thema Internet der Dinge (engl. IoT, Internet of Things). In den ersten Kapiteln werden grundlegende Informationen über IoT präsentiert. Danach folgt die Beschreibung des im IoT am häufigsten eingesetzten Internetprotokolls IPv6, der wichtigsten Anwendungen, des jetzigen Zustands auf dem Markt und der Technologien, welche die Existenz von IoT an sich erlauben. Schließlich werden die wesentlichsten künftigen Herausforderungen behandelt.

ZIELE

Nach dem Durcharbeiten dieses Moduls werden die Studenten die Grundlagen des IoT verstehen und eine Übersicht der Möglichkeiten und Anwendungen in dieser Umgebung haben.

LITERATUR

[1] R. H. Weber (2010). „Internet of Things - New Security and Privacy Challenges“. Computer Law & Security Review 26: 23-30.

[2] Dave Evans (2011). How the Next Evolution of the Internet Is Changing Everything. Cisco Internet of Things White Paper.

[3] Stephen E. Deering and Robert M. Hinden (1998). RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.

[4] Charith Perera et. al. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transactions on Emerging Telecommunications Technology 25 (1): 81–93.

[5] Ma HD. (2011). „Internet of things: Objectives and scientific challenges“. Journal of computer science and technology 26 (6): 919-924.

[6] In Lee and Kyoochun Lee (2015) „The Internet of Things (IoT): Applications, investments, and challenges for enterprises“, *Business Horizons*, 58, 431-440.

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.

[8] Ala Al-Fuqaha et al. (2015) „Internet of Things: A survey on enabling technologies, protocols and applications“, *IEEE Communications Surveys & Tutorials*. DOI 10.1109/COMST.2015.2444095

[9] The European Technology Platform on Smart Systems Integration (2008). „Internet of Things in 2020: A Roadmap for the future“

Inhaltsverzeichnis

1 Was ist das Internet der Dinge (IoT)? Definition, Geschichte und Eigenschaften des IoT

Dieses Kapitel beschreibt wichtige Meilensteine in der Geschichte des **IoT** (*Internet der Dinge*, engl. *Internet of Things*). Zurzeit erlaubt die internetbasierte Informationsarchitektur den Austausch von Dienstleistungen und Waren unter allen Elementen, Geräten und Objekten im Netz. IoT bezieht sich auf die vernetzte Verbindung zwischen alltäglichen Dingen, die häufig auch mit einer Intelligenz ausgestattet sind. In diesem Kontext kann das Internet auch eine Plattform für Geräte sein, die mit der Welt um sie herum elektronisch kommunizieren und Informationen teilen. So kann IoT als eine reale Evolution von allem betrachtet werden, was man sich unter dem Begriff Internet vorstellt, und zwar durch Ergänzung einer größeren Vernetzbarkeit, einer besseren Wahrnehmung der bereitgestellten Informationen und der umfangreichen smarten Dienste. In der Vergangenheit wurde das Internet für verbindungsorientierte Anwendungsprotokolle wie **HTTP** (*Hypertext Transfer Protocol*) und **SMTP** (*Simple Mail Transfer Protocol*) verwendet. Zusätzlich kommunizieren heutzutage viele smarte Geräte sowohl miteinander als auch mit weiteren Steuersystemen. Dieses Konzept wird als **M2M** (*Maschine-Maschine-Kommunikation*, engl. *Machine-to-Machine Communication*) bezeichnet.

IoT (*Internet der Dinge*, engl. *Internet of Things*) ist eine neu entstehende globale internetbasierte technische Architektur, welche den Austausch von Waren und Dienstleistungen im Rahmen der globalen Lieferketten-Netzwerke erleichtert und die Sicherheit und die Privatsphäre aller beteiligten Parteien beeinflusst [1].

Die folgenden Meilensteine können als die wichtigsten Punkte der Entwicklung des IoT betrachtet werden:

- Der Begriff „Internet of Things“ wurde erstmalig im Jahre 1999 von Kevin Ashton verwendet, der im Bereich der Netzwerk-**RFID** (Identifizierung mit Hilfe elektromagnetischer Wellen, engl. *Radio Frequency Identification*) und der neu entstehenden Sensortechnologien arbeitete.
- Das IoT an sich entstand jedoch erst zwischen 2008 und 2009 [2].
- Im Jahre 2010 betrug die Anzahl der physischen, regelmäßig ans Internet angeschlossenen Objekte und Geräte ungefähr 12,5 Milliarden. Zurzeit gibt es etwa 25 Milliarden Geräte, die ans IoT angeschlossen sind - dies entspricht etwa drei Geräte pro Person [2].
- Die Anzahl der smarten, ans IoT angeschlossenen Geräte oder „Dinge“ soll noch auf 50 Milliarden im Jahre 2020 steigen.

Das IoT bringt eine gravierende Änderung in der Lebensqualität, weil es viele neue Möglichkeiten beispielsweise betreffend den Datenzugriff oder die spezifischen Dienstleistungen im Bereich Ausbildung, Sicherheit, Gesundheitswesen oder Transport eröffnet. Andererseits stellt es für Firmen einen der Schlüssel zur

Produktivitätserhöhung wegen des Angebotes des breitverteilten und lokal intelligenten Netzwerks der smarten Geräte und der neuen Dienstleistungen dar, die gemäß Kundenwünschen personalisiert werden können. Das IoT bietet viele Vorteile dank dem verbesserten Management und der Verfolgung von Vermögensgegenständen und Produkten, es kann mit einer großen Datenmenge arbeiten und erlaubt die Optimierung der Einrichtungen und eine effektive Ausnutzung von Ressourcen. Daher kann die Verwendung von IoT Kosteneinsparungen bringen. Darüber hinaus ermöglicht es die Erzeugung von neuen smarten verbundenen Geräten und neuen Geschäftsmodellen.

2 IPv6

Dieses Kapitel stellt die Grundlagen des für IoT erforderlichen Protokolls **IPv6** (*Internet Protocol Version 6*) vor.

2.1 Einführung in IPv6

Verwendet man das Internet für E-Mails, Datenübertragung, Browsen im Web, Herunterladen von Dateien, Bildern oder Videos oder für alle weitere Dienste oder Anwendungen, braucht die Kommunikation zwischen den Netzwerkelementen und dem individuellen Computer, Laptop oder Smartphone das Internetprotokoll (**IP**, engl. *Internet Protocol*), womit das technische Format der Pakete und das Adressierungssystem für alle im Netz kommunizierenden Geräte definiert wird.

Das **IPv6** (*Internet Protocol Version 6*) ist die neueste Version des Kommunikationsprotokolls, das ein System der Identifikation und Lokalisierung für Computer im Netz darstellt und das zum Routing des Datenverkehrs im Internet dient.

Für den Anschluss eines Gerätes ans Internet muss ihm eine IP-Adresse zugeteilt werden. Die erste Version des öffentlich eingesetzten Internetprotokolls war **IPv4** (*Internet Protocol Version 4*). Dieses Protokoll wurde von **DARPA** (*Defense Advanced Research Projects Agency*) entwickelt. Diese Behörde des Verteidigungsministeriums der Vereinigten Staaten wurde im Jahre 1958 gegründet und ist für die Entwicklung von neuen Technologien vor allem für Militäranwendungen verantwortlich. IPv4 arbeitet mit einem System aus nummerischen Adressen mit 32 Bits. Gerade die Länge von 32 Bits begrenzt die gesamte Anzahl der verwendbaren Adressen auf ungefähr 4,3 Milliarden für alle weltweit ans Internet angeschlossenen Geräte. Bald schon gab es mehr Geräte als verfügbare Adressen. Daher fing die Internettechnik-Arbeitsgruppe **IETF** (*Internet Engineering Task Force*), die sich mit der Erstellung von Standards fürs Internet beschäftigt, schon im Jahre 1998 mit der Arbeit auf der neuen Version des IP an. Das IPv6, Nachfolger des IPv4, wurde zuerst im Dokument RFC 2460 formal beschrieben [3].

IPv6 verwendet ein 128-Bit-Adressformat und daher kann die Gesamtanzahl der Adressen 2^{128} (ungefähr $3{,}4 \cdot 10^{38}$) betragen, d. h. $8 \cdot 10^{28}$ mal mehr als IPv4. Neben der Vergrößerung des Adressraums, als einer der wesentlichsten Vorteile des IPv6, gibt es auch weitere wichtige technologische Änderungen in IPv6: eine einfachere Verwaltung, das bessere Multicast-Routing, das effizientere Routing im Allgemeinen, das einfachere Headerformat, die integrierte Authentifizierung und die Unterstützung der Privatsphäre.

Das IPv6 wird schrittweise eingeführt und mit dem älteren IPv4 eine Zeit lang koexistieren. Die Kundengeräte, Netzwerkelemente, Anwendungen, Inhalt und Dienste werden an das neue Internetprotokoll IPv6 angepasst. Darüber hinaus wird der Übergang vom IPv4 auf IPv6 eine gemeinsame Gruppe von Standards für Firmen, Bildungssysteme u. a. weltweit einführen.

Eine IPv6-Adresse stellt acht Gruppen mit je vier hexadezimalen Zeichen dar, die mit einem Doppelpunkt getrennt werden. Weil die Adresse ziemlich lang ist, kann diese vollständige Schreibweise auch auf verschiedene Weisen verkürzt werden. Das Headerformat des IPv6 ist auf dem Bild 1 gezeigt.

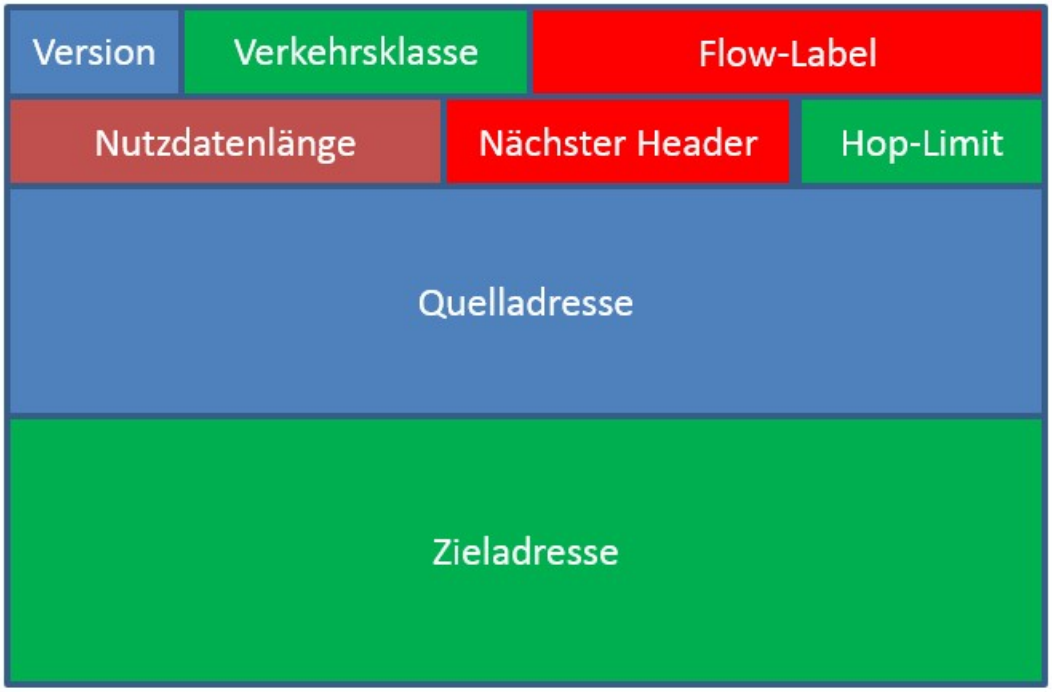


Abb. 1. Headerformat des IPv6 [3]

Struktur des Headerformats des IPv6	
Version	4 Bits, Version des Internetprotokolls = 6
Verkehrsklasse	8 Bits
Flow-Label	20 Bits
Nutzdatenlänge	16 Bits, unsignierte ganze Zahl, die Länge des Blocks der Nutzdaten, d. h. des Restes des Pakets nach diesem Header, in Oktetten
Nächster Header	8 Bits, Selektor zur Identifikation des Headertyps gleich nach diesem IPv6-Header, es werden die gleichen Werte wie beim IPv4 verwendet
Hop-Limit	8 Bits, positive ganze Zahl, bei jedem Durchgang des Pakets durch Netzknoten um 1 vermindert, beim Null des Hop-Limits wird das Paket verworfen
Quelladresse	128 Bits, Adresse des Paketabsenders
Zieladresse	128 Bits, Adresse des geplanten Empfängers des Pakets (wenn es einen Routingheader gibt, muss es sich nicht um den letzten Empfänger handeln)

Die wichtigsten vom IPv6 eingeführten Neuigkeiten sind: ein neues Headerformat, eine effiziente und hierarchische Adressierungs- und Routinginfrastruktur, ein größerer Adressraum und eine Adresskonfiguration sowohl ohne und mit Adressen, die IP-Sicherheit, die Erweiterungsmöglichkeit, eine bessere Unterstützung der Dienstgüte (**QoS**) und ein neues Protokoll für Interaktion von benachbarten Knoten.

Das IPv6 löste einige Sicherheitsprobleme der IPv4-Netze durch Einführung der obligatorischen (heutzutage schon wählbaren) IP-Sicherheit **IPsec** (engl. *IP Security*). Daher ist IPv6 viel effizienter. IPsec verbessert das ursprüngliche IP durch Sicherstellung der Authentizität, Integrität, Vertraulichkeit und Zugriffskontrolle für jedes IP-Paket mittels der Protokolle **AH** (*Authentication Header*) und **ESP** (*Encapsulating Security Payload*). Darüber hinaus bedeutet die Vergrößerung der Bitanzahl im Adressfeld auf 128 Bits ein bedeutsames Hindernis für Angreifer, die ein komplexes Port-Scanning planen. Andererseits kann ein öffentlicher Schlüssel mit der IPv6-Adresse verbunden werden: dann spricht man über eine kryptographisch generierte Adresse (engl. **CGA**, *Cryptographically Generated Address*).

IPv6 garantiert auch eine höhere Sicherheit des mobilen Anschlusses. Obwohl das MobileIP schon in IPv4 zur Verfügung stand, handelt es sich beim IPv6 im Unterschied zum IPv4 um eine integrierte, nicht nur ergänzte Funktionalität. Dies bedeutet, dass jeder IPv6-Knoten nach Bedarf ein mobiles IP verwenden kann. Das mobile IPv6 verwendet im Header zwei Erweiterungen: einen Routingheader zur Registrierung und einen Zielheader zur Zustellung der Daten zwischen den mobilen Knoten und den entsprechenden festen Knoten.

3 IoT-Anwendungen

In diesem Kapitel werden einige wichtige Anwendungen aus dem Bereich IoT beschrieben. Auch werden grundlegende Elemente der IoT-Architektur und die erwartete Entwicklung auf dem Markt vorgestellt.

3.1 Einführung

IoT kann als eine Kombination von Sensoren und Aktoren betrachtet werden, welche spezifische Angaben bieten und empfangen - diese Angaben werden weiter digitalisiert und in beide Richtungen mittels Kommunikationsnetzen übertragen, so dass sie von vielen verschiedenen Diensten und Endbenutzern verwendet werden können [4].

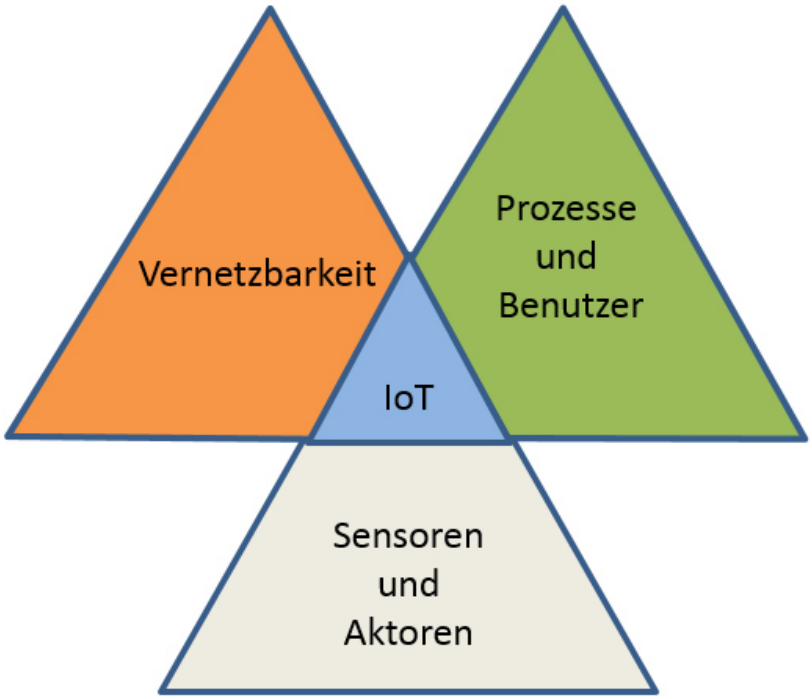


Abb. 2. IoT-Konzept

An ein Objekt oder Gerät können viele Sensoren angeschlossen werden, die dann eine breite Skala von physikalischen Größen oder Ereignissen messen können und nachfolgend die erworbenen Daten in eine Cloud übertragen können. Eine solche Messung kann als ein Dienstmodell betrachtet werden.

Klassifikation der Sensoren	
Anbieter der Sensordaten	Geschäftseinheiten, welche die Sensoren selbst einsetzen und verwalten.
Organisationen	Öffentliche oder private. Öffentliche Infrastruktur. Kommerzielle Organisationen. Private Unternehmen. Anbieter von Technologien und Dienstleister.
Personen und Haushalte	Handys, Smartwatches, Gyroskope, Kameras, GPS, Beschleunigungssensoren, Mikrofone, Laptops, Haushaltsgegenstände (z. B. Fernseher, Kameras, Gefriertruhen, Mikrowellenherde, Waschmaschinen, smarte Haushaltsgeräte).

Moderne Geräte, z. B. Kühlschränke oder Fernseher, werden mit Kommunikations- und Sensorsystemen ausgestattet. Diese Fähigkeiten werden noch weiter erweitert, weil noch smartere Technologien eingesetzt werden.

Möglichkeiten der verbundenen smarten Geräte	
Überwachung	Außenumgebung. Zustand, Betrieb und Ausnutzung des Produktes.
Steuerung	Steuerung der Funktionen des Produktes. Personalisierung der Benutzereinstellungen. Programmierung.
Optimierung	Prädiktive Diagnostik. Optimierung der Leistung des Produktes. Kostenreduzierung.
Autonomie	Autonome Verbesserung und Personalisierung des Produktes. Eigendiagnostik und Selbstreparaturen. Koordination des Betriebes mit weiteren Produkten.
Effizienter Entscheidungsprozess	Echtzeitdaten für richtige Entscheidungen.

Die Architektur der IoT-Systeme kann in vier Schichten eingeteilt werden: Sensorik, Datenaustausch, Informationsintegration und Anwendungsdienste [5].

Smarte Geräte können schon über einen üblichen Internetanschluss verbunden werden. IoT umfasst jedoch auch die Schicht der Sensorik, welche die Anforderungen an die Fähigkeiten dieser Geräte reduziert und ihre gegenseitige Verbindung erlaubt. Die Empfänger der Sensordaten kommunizieren mit den Sensoren oder ihren Inhabern in der Schicht der Informationsintegration, die für die Kommunikation und Transaktionen verantwortlich ist. Inzwischen tauchen neue Anforderungen und Herausforderungen an Datenaustausch, Informationsfilterung und -integration, Definitionen neuer Dienste für Benutzer und komplexere Netzwerkarchitekturen auf. Darüber hinaus steigt die Verwendung der Cloud-Technologien exponentiell. Neue Infrastrukturplattformen und Softwareanwendungen werden im Rahmen des IoT angeboten. Zu den Hauptvorteilen des IoT gehört die Erzeugung von innovativen effizienteren Diensten und Mehrwertlösungen, Kostenreduzierung der Datenerfassung für die

bestehenden Dienste und die Möglichkeit der neuen Einkommensquellen im Rahmen eines zukunftsfähigen Geschäftsmodells. Diese Anwendungen können an Kunden, Geschäften, Werbung und Marktuntersuchung, industrielle und wissenschaftliche Öffentlichkeit durch eine richtige Anweisung der Entwickler orientiert werden.

IoT-Architektur mit vier Schichten	
Sensorik-Schicht	Aufnehmen und Erfassen von Daten aus physischen Objekten.
Datenaustauschschicht	Transparente Datenübertragung mittels Kommunikationsnetzen.
Informationsintegrationsschicht	Verarbeitung der unsicheren Informationen von Netzen, Filterung der unerwünschten Daten und Transformation der wichtigsten Informationen in nutzbare Kenntnisse für Dienste und Endbenutzer.
Anwendungsdienstschicht	Bereitstellung von Inhaltsdiensten den Endbenutzern.

3.2 IoT-Markt

IoT ist eine neu entstehende globale internetbasierte technische Architektur, welche den Austausch von Waren und Dienstleistungen im Rahmen der globalen Lieferketten-Netzwerke erleichtert [1]. Um den technologischen Trend immer schnellere Datenraten und niedrigere Verzögerungen der Übertragung zu erreichen, wird die Verdoppelung der Größe des Internets jede 5,3 Jahre angenommen und das Cloud Computing kann eine entscheidende Rolle in dieser Entwicklung spielen. Das Cloud Computing ist eine der Plattformen, die für die Unterstützung des IoT kritisch sind. Die meisten „Dinge“ der realen Welt werden in die virtuelle Welt dank einer Möglichkeit des vollständigen Internetanschlusses jederzeit und überall integriert.

Das **Cloud Computing** ist ein Modell für einen Zugriff auf einen gemeinsam genutzten Pool an konfigurierbaren Computerressourcen, das es den Benutzern erlaubt, Vorteile aus den bestehenden Technologien zu nutzen, ohne dass fundierte Kenntnisse oder Erfahrung erforderlich sind.

Im Jahre 2010 betrug die Anzahl der physischen, regelmäßig ans Internet angeschlossenen Objekte und Geräte ungefähr 12,5 Milliarden. Es wird geschätzt, dass diese Zahl auf 25 Milliarden im Jahre 2015 durch mobile Geräte und bis 2020 weiter auf 50 Milliarden steigen wird [2].

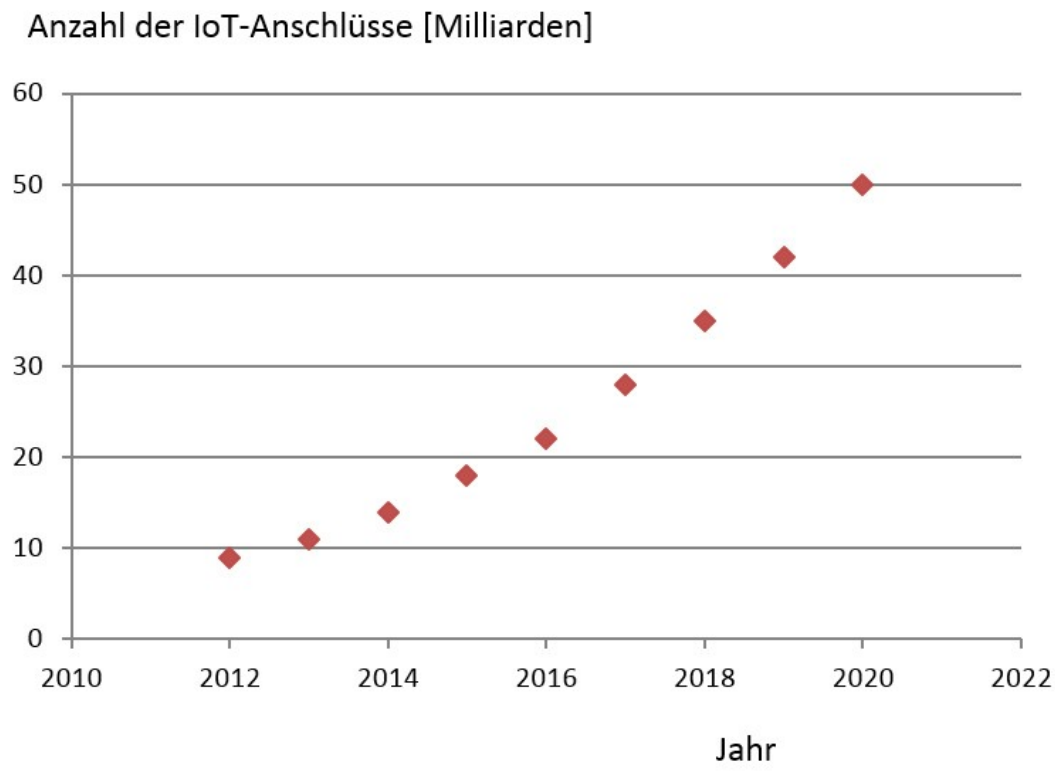


Abb. 3. Anzahl der IoT-Anschlüsse [2]

Die vernetze Welt	
31 %	Telefone
29 %	Notebooks
10 %	Smartphones
8 %	Smart-TV
5 %	Tablets
5 %	Spielkonsolen
5 %	Multimedia-Spieler
5 %	E-Book-Readers
3 %	Weitere Geräte

Die größte Anzahl der M2M-Verbindungen befindet sich zurzeit in Asien, vor allen wegen der großen Anstrengungen einigen Staaten wie Japan und China. Die amerikanischen und europäischen Technologieunternehmen machen jedoch auch wichtige Fortschritte im Bereich des IoT und daher kann auch ein Einstieg der Anzahl der Anschlüsse erwartet werden. In Anknüpfung an die Entstehung eines so wichtigen Phänomens wie IoT müssen neue Regulierungsansätze definiert werden, so dass die Privatsphäre und die Sicherheit der Benutzer und der Daten sichergestellt werden.

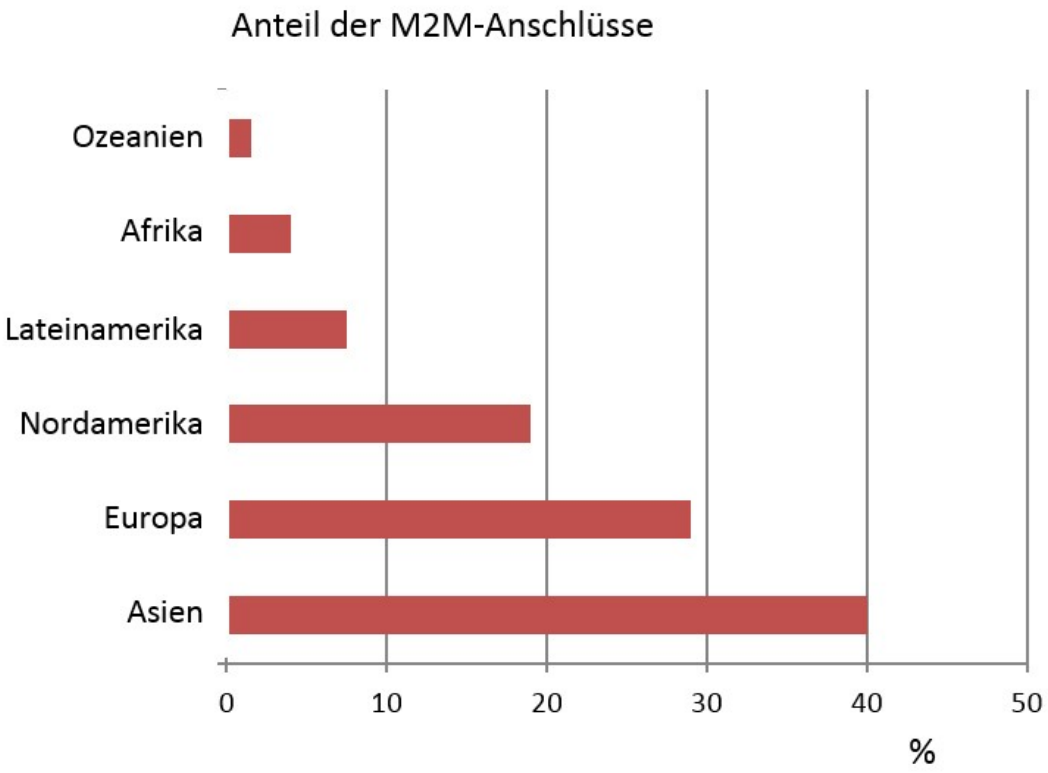


Abb. 4. Anteil der M2M-Anschlüsse [2]

3.3 Anwendungen

Das IoT kann eine praktisch unbegrenzte Anzahl von Anwendungen und Diensten anbieten, welche für viele Bereiche der menschlichen Tätigkeit angepasst werden können und welche das Leben erleichtern und seine Qualität erhöhen. Dieses Kapitel bietet eine kurze Auflistung und grundlegende Beschreibung der IoT-basierten Anwendungen und Dienste. Bis 2020 sollen diese Anwendungen und Dienste im Bereich IoT den Wert von 19 Billionen Dollar erreichen.

IoT-Anwendungen und Dienste:

- Angeschlossene intelligente Gebäude: Verbesserung der Effizienz (Energiemanagement und -einsparung) und Sicherheit (Sensoren und Alarmanlagen). Haustechnische Anwendungen einschließlich smarter Sensoren und Aktoren zur Steuerung der Haushaltsgeräte. Gesundheits- und Ausbildungsdienste für Haushalte. Fernbedienung der Behandlungen für Patienten. Kabel-/Satellitendienste. Systeme der Energiespeicherung/-erzeugung. Automatisches Ausschalten der Elektronik, wenn sie nicht verwendet wird. Smarte Thermostate. Rauchmelder. Anwendungen der Zutrittskontrolle (für Gebäude und Räume). Smarte Türschlösser. In Gebäudeinfrastruktur integrierte Sensoren für Rettungs- und Bereitschaftsdienste. Sicherheit für alle Familienmitglieder.

- Smarte Städte und Transportsysteme: Integration der Sicherheitsdienste. Optimierung des öffentlichen und privaten Verkehrs. Parksensoren. Smarte Verwaltung der Parkdienste und des Verkehrs in Echtzeit. Smartes Management der Ampeln in Abhängigkeit von Staus. Identifikation von Fahrzeugen, welche die erlaubte Parkzeit überschreiten. Intelligente Energienetze (Smart Grids). Sicherheit (Kameras, smarte Sensoren, Informationen für Bürger). Wasserwirtschaft. Bewässerung von Parks und Gärten. Smarte Mülltonnen. Kontrolle der Verschmutzung und Mobilität. Erfassung einer sofortigen Rückkopplung und Meinungen von Bürgern. Smart Governance. Wahlsysteme. Überwachung von Unfällen, Koordination von Notfallmaßnahmen.

Abb. 5. Beispiel der IoT-Anwendungen: Smarte Städte

- Ausbildung: Verbindung der virtuellen und physischen Klassenzimmer zur Sicherstellung einer effizienteren und erreichbareren Bildung, E-Learning. Dienste des Zugriffs auf virtuelle Bibliotheken und Bildungsportale. Austausch von Berichten und Ergebnissen in Echtzeit. Lebenslanges Lernen. Fremdsprachenlernen. Anwesenheitsmanagement.

- Unterhaltungselektronik: Smartphones, Smart-TV, Laptops, Computers und Tablets. Smarte Kühlschränke, Geschirrspülmaschinen und Wäschetrockner. Smartes Heimkinosystem. Smarte Haushaltsgeräte. Sensoren für Tierhalsbänder. Personalisierung der Benutzererfahrung. Autonomer Betrieb der Produkte. Personenortungsgeräte. Smarte Brillen.

- Gesundheitswesen: Überwachung von chronischen Krankheiten. Verbesserung der Qualität der Behandlung und des Lebens für Patienten. Activity Tracker. Ferndiagnostik. Ans Internet angeschlossene Armbänder. Interaktive Gürtel. Überwachung von sportlichen Aktivitäten. Intelligente Tags für Drogen. Kontrolle des Arzneimittelgebrauchs. Biochips. Hirn-Computer-Schnittstellen. Überwachung der Essgewohnheiten.

- Autoindustrie: Smarte Autos. Verkehrssteuerung. Fortgeschrittene Diagnostik der defekten Bestandteile. Drahtlose Überwachung des Reifendrucks. Smartes Energiemanagement und Verbrauchssteuerung. Eigendiagnostik. Beschleunigungssensoren. Sensoren zur Messung der Position, Anwesenheit

und Näherung. Analyse des optimalen Wegs zum Ziel in Echtzeit. GPS-Ortung. Steuerung der Fahrzeuggeschwindigkeit. Autonome Fahrzeuge mit IoT-Diensten.

- Landwirtschaft und Umwelt: Messung und Überwachung der Umweltverschmutzung (CO_2, Geräusch, Fremdstoffe in der Umwelt). Vorhersage der Klimaänderungen mittels smarter Sensoren. Passive RFID-Tags an landwirtschaftlichen Produkten. Sensoren in Produktpaletten. Abfallwirtschaft. Bestimmung der Ernährungswerte.

- Energiedienstleistungen: Exakte Daten über Energieverbrauch. Smarte Messung. Intelligente Energienetze (Smart Grids). Analyse und Vorhersage des Verhaltens und der Muster des Energieverbrauchs. Prädiktion der künftigen Energietrends und Bedürfnisse. Drahtlose Sensornetze. Energieernte und -verwertung.

- Smarte Vernetzbarkeit: Datenmanagement und Bereitstellung von Diensten. Einsatz von sozialen Medien und Social-Networking. Zugriff auf E-Mail, Sprach- und Videodienste. Interaktive Gruppenkommunikation. Echtzeit-Streaming. Interaktive Spiele. Augmented Reality. Überwachung der Netzwerksicherheit. Tragbare Benutzerschnittstellen. Affective Computing. Biometrische Authentifizierungsverfahren. Benutzertelematik. M2M-Kommunikationsdienste. Big-Data-Analyse. Virtual Reality. Dienste des Cloud Computings. Ubiquitäres Computing. Computervision. Smarte Antennen.

- Fertigung: Durchflusssensoren für Gase und Flüssigkeiten. Smarte Feuchtigkeits-, Temperatur-, Bewegungs-, Kraft-, Last-, Leck-/Pegelsensoren. Maschinelles Sehen. Wahrnehmung von Geräuschen und Schwingungen. Kombinierte Anwendungen. Smarte Steuerung von Roboten. Steuerung und Optimierung der Fertigungsprozesse. Mustererkennung. Maschinelles Lernen. Prädiktive Analyse. Mobile Logistik. Lagerverwaltung. Verhinderung von Überproduktion. Effiziente Logistik.

- Einkauf: Intelligentes Einkaufen. RFID und weitere elektronische Tags und Lesegeräte. Barcodes im Einzelhandel. Bestandskontrolle. Kontrolle des geografischen Ursprungs von Lebensmitteln und weiteren Produkten. Kontrolle der Lebensmittelqualität und -sicherheit.

4 Basistechnologien

Das IoT-Konzept kann sich in der realen Welt dank Fortschritten in den unterliegenden Technologien geltend machen. In diesem Kapitel werden die relevantesten Basistechnologien behandelt, so dass ihre wahrscheinliche Rolle im künftigen IoT besser vorgestellt werden kann [6, 7].

4.1 Energie

Die Energiespeicherungstechnologien stellen einen Wegbereiter der Einführung der IoT-Anwendungen dar. Die Energiethemen in allen ihren Phasen, ab Energieernte (engl. Energy Harvesting) und -erzeugung zum Energieverbrauch, sind entscheidend für die Entwicklung des IoT. Diese Technologien sollen Lösungen der Erzeugung und Ernte der Energie mit einer hohen Dichte bereitstellen. Diese Lösungen werden dann in Kombination mit heutiger Kleinleistung-Nanoelektronik den Entwurf von intelligenten, sensorbasierten, drahtlos identifizierbaren Geräten mit eigener Stromquelle ermöglichen. Die Forschung und Entwicklung in diesem Bereich (Nanoelektronik, Halbleitertechnologien, Sensortechnik, Integration von Mikrosystemen) sind immer noch erforderlich, wobei das Ziel Geräte mit einem ultraniedrigen Verbrauch und effizientere und kompaktere Energiespeicher wie Batterien, Brennstoffzellen und gedruckte Batterien / Polymerbatterien sind, weil die gegenwärtigen Geräte den künftigen Kriterien der erforderlichen Rechenleistung und des begrenzten Energieverbrauchs nicht entsprechen. Außerdem wird die Systemintegration die Effizienz der bestehenden Systeme steigern und eine Reihe von Lösungen für die zukünftigen Bedürfnisse anbieten.

4.2 Sensoren

Sensoren sind einer der wichtigsten Bausteine des IoT. Als ubiquitäre Systeme können sie praktisch überall eingesetzt werden. Sie können auch unter die menschliche Haut implantiert werden oder in eine Brieftasche oder in ein T-Shirt installiert werden. Einige Sensoren messen nur vier Millimeter, aber die erfassten Daten können Hunderte von Kilometern weit weg empfangen werden. Sie ergänzen die menschlichen Sinne und wurden in vielen Industrien unentbehrlich, vom Gesundheitswesen bis zum Maschinenbau. Sensoren haben den unbestrittenen Vorteil, dass sie menschliche Bedürfnisse basierend auf Kontextinformationen von ihrer Umgebung vorhersagen können. Ihre Intelligenz, mit zahlreichen Netzwerken multipliziert, ermöglicht nicht nur das Berichten über die externe Umgebung, sondern auch das Handeln ohne menschlichen Eingriff.

Miniaturisierte Silizium-Chips werden mit neuen Fähigkeiten in einer kleineren Form und mit besserer Verarbeitungsleistung und Effizienz entworfen. Die Kosten sinken in Übereinstimmung mit dem mooreschen Gesetz. Auch die Kosten der Bandbreite und die Verarbeitungskosten wurden reduziert - daher können mehr Geräte nicht nur miteinander verbunden, sondern auch mit einer ausreichenden Intelligenz ausgestattet werden, so dass sie sowohl die generierten als auch die empfangenen Daten richtig verarbeiten können.

Solche Fähigkeiten wie Kontextbewusstsein und gegenseitige Kommunikation zwischen Maschinen erhalten eine hohe Priorität für die IoT-Technologie. Weitere Prioritäten umfassen die Integration des Speichers und der Rechenleistung, die Beständigkeit gegen raue Umgebungsbedingungen und eine bezahlbare Sicherheit. Ein Befähigungsfaktor ist auch die Entwicklung von Prozessor-/Mikrocontrollerkernen mit einem ultraniedrigen Stromverbrauch, die spezifisch für mobile IoT-Dienste und die neue Klasse von einfachen und erschwinglichen smarten Systemen für IoT bestimmt werden. Die Lösungen in dieser Hinsicht werden von Mikroprogramm-Zustandsmaschinen bis Mikrocontrollern reichen. Die eigentliche Wahl ist dann ein Kompromiss zwischen Flexibilität, Programmierbarkeit, Chipfläche und Energieverbrauch. Diese Geräte erfordern eine Form des nichtflüchtigen Speichers (EEPROM/FRAM/Polymer), sei er bei der Fertigung lasergetrimmt, einmalig programmierbar oder elektrisch wiederbeschreibbar. Wiederbeschreibbare nichtflüchtige Speicher werden eindeutig bevorzugt, weil sie einen hohen Durchsatz bei den Produktionsprüfungen erreichen und weil sie die Funktionen eines Benutzerspeichers, eines programmierbaren Speichers und eines Speichers für Sensordaten kombinieren.

4.3 Cloud Computing

Das Cloud Computing ist ein Modell für einen auf Abruf verfügbaren Zugriff auf konfigurierbare Ressourcen (z. B. Computer, Netzwerke, Server, Speicher, Anwendungen und Dienste, Software), und zwar in der Form entweder einer Infrastruktur als Dienst (**IaaS**, *Infrastructure as a Service*) oder Software als Dienst (**SaaS**, *Software as a Service*). Eine der wichtigsten Folgen der Einführung des IoT ist die riesige Menge von Daten, die von den ans Internet angeschlossenen Geräten generiert werden [7]. Viele IoT-Anwendungen erfordern massive Datenspeicher, enorme Verarbeitungsgeschwindigkeit wegen der Echtzeitentscheidungen und Hochgeschwindigkeits-Breitbandnetzwerke für das Streaming von Daten, Audio oder Video. Cloud Computing bietet eine ideale Backend-Lösung für die Manipulation mit riesigen Datenstreams und ihre Echtzeitverarbeitung für eine beispielslose Anzahl von IoT-Geräten und Menschen.

4.4 Kommunikation

Neue smarte Multibandantennen, die in einem Chip integriert werden und aus neuen Materialien hergestellt werden, sind die Kommunikationsmittel, welche die gegenseitige Kommunikation der Geräte ermöglichen. Antennen auf Chips müssen für die Größe, Kosten und Effizienz optimiert werden und können wegen ihres Einsatzes von verschiedenen Substraten und 3D-Strukturen in vielen Formen erhältlich werden: Spulen auf Chips, gedruckte Antennen, eingebettete Antennen und Mehrfach-Antennen. Weil energiesparende Kommunikationsprotokolle für Multibandübertragungen eingesetzt werden sollen, müssen auch die Fragen der verwendeten Modulationsverfahren und Übertragungsraten gelöst werden. Die Kommunikationsprotokolle werden für weborientierte Architekturen der IoT-Plattform entworfen, wo alle Objekte, drahtlose Geräte, Kameras, PCs usw. kombiniert werden, um den Ort, die Absicht und sogar Emotionen via Netzwerk analysiert werden können. Man braucht neue Verfahren einer wirksamen Verbrauchssteuerung auf verschiedenen Ebenen des Netzwerkes, von Netzwerk-Routing bis zur Architektur der individualen Geräte.

4.5 Integration

Die Integration intelligenter Einrichtungen in eine Verpackung oder noch besser in die Produkte an sich erlaubt wesentliche Kosteinsparungen und erhöht die Umweltfreundlichkeit der Produkte. Die Trends der Integration von Chips und Antennen in atypische Substrate wie Textilien und Papier, der Entwicklung neuer Substrate, Leiterbahnen und Bindemittel, die für raue Umgebungsbedingungen und umweltfreundliche Entsorgung geeignet sind, werden fortdauern. Die Technologie **SiP** (engl. *System-in-Package*) erlaubt eine flexible 3D-Integration verschiedener Elemente wie Antennen, Sensoren, aktiven und passiven Komponenten in die Verpackung, die Verbesserung der Leistung und die Reduzierung der Kosten. RFID-Inlays werden zur Verbindung der Chips und Antennen in einem integrierten Schaltkreis verwendet, so dass eine breite Auswahl von Formen und Größen der Etiketten erzeugt werden kann, die nicht mehr nachträglich montiert werden müssen.

4.6 Standards

IoT-Geräte sind sehr mannigfaltig und können verschiedenste Parameter gemäß unterschiedlichen Normen in diversen Einheiten messen. Obwohl immer noch konkurrierende proprietäre Protokolle vorgeschlagen werden, ist es wahrscheinlich, dass Open Source Standards einen der Wege zur Interoperabilität darstellen werden.

Es ist offensichtlich, dass offene Standards der entscheidende Befähigungsfaktor für den Erfolg der drahtlosen Kommunikationstechnologien und im Allgemeinen aller Maschine-Maschine-Kommunikation sind. Für den Einsatz von IoT-Anwendungen ist jedoch eine schnellere Einführung von interoperablen Standards notwendig. Es müssen Anforderungen der eindeutigen globalen Identifikation, der Zuteilung von Namen und Resolver aufgeklärt werden. In der Zukunft müssen die Fragen der mangelnden Konvergenz der Definition von allgemeinen Referenzmodellen, Referenzarchitektur für Zukunftsnetze (engl. Future Networks), Zukunftsinternet (engl. Future Internet) und IoT und die Integration älterer Systeme und Netzwerke gelöst werden.

5 Herausforderungen und Hindernisse des IoT

Man muss sich noch mit vielen Herausforderungen befassen. Die richtigen Lösungen werden es den Dienstleistern und Anwendungsprogrammierern erlauben, ihre Produkte effizient zu implementieren. Weiter werden die grundlegenden Herausforderungen der Entwicklung und Einführung des IoT beschrieben [8].

5.1 Herausforderungen

Zuverlässigkeit

Die Zuverlässigkeit ist das Ziel, die Erfolgsrate der Bereitstellung der IoT-Dienste zu erhöhen. Sie ist mit Verfügbarkeit eng verbunden, weil mittels Zuverlässigkeit die Verfügbarkeit von Informationen und Dienstleistungen sichergestellt wird. Die Zuverlässigkeit ist noch wichtiger und hat strengere Anforderungen im Bereich der Notfallanwendungen. Ein Schlüsselteil dieser Systeme ist das Kommunikationsnetzwerk, das beständig gegenüber Versagen sein muss, um eine zuverlässige Verteilung von Information zu garantieren. Die Zuverlässigkeit muss in der Soft- und Hardware in allen IoT-Schichten implementiert werden. Für einen effizienten Betrieb des IoT muss die unterstützende Kommunikation zuverlässig sein, weil beispielsweise eine unzuverlässige Datenwahrnehmung, -erfassung, -verarbeitung oder -übertragung zu großen Verzögerungen, Datenverlusten und sogar zu falschen Entscheidungen führen können - dies kann sich in katastrophale Folgen und infolgedessen in Betriebsunsicherheit des IoT auswirken.

Die **Zuverlässigkeit** bedeutet eine richtige Funktion des Systems im Einklang mit seiner Spezifizierung.

Leistungsfähigkeit

Die Bewertung der Leistungsfähigkeit der IoT-Dienste ist eine große Herausforderung, weil sie von der Leistungsfähigkeit vieler Komponenten und der unterliegenden Technologien abhängt. IoT und andere Systeme, müssen sich ständig entwickeln und die Dienste verbessern, so dass Anforderungen der Kunden erfüllt werden. Auch der Zustand der IoT-Geräte muss überwacht und ausgewertet werden, so dass die bestmögliche Leistung für einen erschwinglichen Preis für Kunden angeboten werden kann. Für die Bewertung der Leistungsfähigkeit des IoT können viele Metriken eingesetzt werden – unter anderen Geschwindigkeit des Prozessors, Kommunikationsgeschwindigkeit, Ausführung des Gerätes und sein Preis.

Die Bewertung der Leistungsfähigkeit der einzelnen unterliegenden Protokolle und Technologien, Protokolle der Anwendungsschicht und QoS ist in der Literatur beschrieben, aber eine gründliche Bewertung der Leistungsfähigkeit der IoT-Anwendungen fehlt noch.

Die Dienstgüte (engl. **QoS**, *Quality of Service*) ist die Gesamtleistungsfähigkeit eines Telefon- oder Computernetzwerks, vor allem aus der Sicht des Benutzers.

Interoperabilität

Eine weitere Herausforderung für IoT ist die Ende-zu-Ende-Interoperabilität, weil eine große Menge von heterogenen Dingen auf verschiedenen Plattformen

behandelt werden müssen. Die Interoperabilität soll sowohl von Anwendungsentwicklern als auch Herstellern der IoT-Geräte beachtet werden, so dass die Dienste für alle Kunden ohne Rücksicht auf die Spezifizierungen ihrer Hardwareplattform vorbereitet werden. Zum Beispiel unterstützen die meisten Smartphones zurzeit die üblichen Kommunikationstechnologien wie Wi-Fi, NFC und GSM, um eine Interoperabilität in unterschiedlichen Umgebungen und Situationen zu garantieren. Daher sollen die Programmierer ihre IoT-Anwendungen so entwerfen, dass neue Funktionalitäten ohne jeden negativen Einfluss auf andere Funktionen ergänzt werden können und die Integration mit verschiedenen Kommunikationstechnologien aufrechterhalten wird. Deshalb ist die Interoperabilität ein signifikantes Kriterium beim Entwurf und bei der Einführung der IoT-Dienste, so dass Anforderungen der Kunden erfüllt werden. Neben vielen Protokollen stellen unterschiedliche Interpretierungen der gleichen Standards ein Problem dar, die von verschiedenen Parteien implementiert werden. Um eine solche Vieldeutigkeit zu vermeiden, soll die gegenseitige Interoperabilität zwischen verschiedenen Produkten beispielsweise mittels ETSI Plugtests geprüft werden. Die Interoperabilität der bewährten IoT-Lösungen kann auch mit Hilfe des Forschungsprojektes PROBE-IT überprüft werden, zum Beispiel mittels CoAP, 6LoWPAN oder des Tests semantischer Interoperabilität des IoT.

Auch wenn zwei Geräte denselben Standard erfüllen, können sie immer noch nicht interoperabel sein. Das ist vielleicht das größte Problem beim breiten Einsatz von IoT-Technologien. Künftige Geräte müssen unterschiedliche Kommunikationsstandards und -protokolle integrieren, welche auf unterschiedlichen Frequenzbändern betrieben werden und welche unterschiedliche zentralisierte oder verteilte Architekturen unterstützen. Auch müssen sie imstande sein, mit anderen Netzwerken zu kommunizieren, bis globale, hochentwickelte Standards erstellt werden.

Sicherheit und Privatsphäre

Die Sicherheit ist eine bedeutende Herausforderung für die IoT-Implementierungen wegen des Mangels an gemeinsamen Standards und Architekturen. In heterogenen Netzwerken wie IoT kann die Sicherheit und Privatsphäre nicht einfach für Benutzer garantiert werden. Die Schlüsselfunktionalität des IoT beruht auf dem Austausch der Informationen zwischen Milliarden oder sogar Billionen von Objekten im Internet. Eine der offenen Fragen in der IoT-Sicherheit, die bisher im Rahmen der Standards nicht behandelt wurde, ist die Verteilung der Schlüssel unter den Geräten. Diese Probleme mit der Privatsphäre und den Operationen des Zugangs zu Profilen zwischen IoT-Geräten ohne unbefugte Eingriffe sind dabei sehr dringend. Daher ist die Sicherstellung des Datenaustauschs notwendig, so dass die Privatsphäre nicht gefährdet wird. Die steigende Anzahl von smarten Geräten, die mit sensiblen Daten arbeiten, erfordert eine transparente und einfache Zugriffskontrolle, so dass zum Beispiel ein Dienstleister nur Daten lesen darf und der andere das Gerät steuern darf. In dieser Hinsicht wurden schon einige Lösungen entworfen, zum Beispiel Gruppierung der eingebetteten Geräte in virtuelle Netzwerke und Zurverfügungstellung der Geräte nur innerhalb dieser einzelnen virtuellen Netzwerke. Eine weitere Möglichkeit ist die Unterstützung der Zugriffskontrolle in der Anwendungsschicht gemäß den einzelnen Dienstleistern.

Management

Die Verbindung von Milliarden oder sogar Billionen smarter Geräte stellt die Dienstleister vor entmutigende Probleme des Fehler-, Konfigurations-, Abrechnungs-, Leistungs- und Sicherheitsmanagements (engl. **FCAPS**; *Fault, Configuration, Accounting, Performance and Security*) dieser Geräte. Dieses Bestreben um Management solcher Aspekte braucht auch die Entwicklung von neuen, einfach verwalteten Protokollen zur Meisterung des Management-Alptraums, der nach ein paar Jahren nach der Einführung des IoT auftreten kann. Ein erfolgreiches Management der IoT-Geräte und -Anwendungen kann zu einem wirksamen Instrument für den Einstieg des IoT werden. Zum Beispiel die Überwachung der M2M-Kommunikation der IoT-Objekte ist zur Sicherstellung einer ununterbrochenen Vernetzbarkeit für die Bereitstellung der auf Abruf geleisteten Dienste wichtig. Der Standard für eine „entlastete“ M2M-Kommunikation (engl. **LWM2M**, *Light-Weight M2M*), der von Open Mobile Alliance entwickelt wurde, hat das Ziel der Erzeugung einer Schnittstelle zwischen M2M-Geräten und M2M-Servern und daher auch eines anwendungsunabhängigen Systems zum Management einer breiten Skala von Geräten. Ein solches System wird es dann den M2M-Anwendungen ermöglichen, die M2M-Geräte, -Dienste und -Anwendungen fern zu verwalten. Das Protokoll NETCONF Light ist ein Produkt der Arbeitsgruppe **IETF** (*Internet Engineering Task Force*) fürs Management der Geräte mit beschränkten Funktionen und definiert Verfahren für die Installation, Änderung und das Löschen der Konfiguration der Netzwerkgeräte. Es kann auch zur Verwaltung eines breiten Spektrums der Geräte von ressourcenbeschränkten bis ressourcenreichen Objekten dienen. Die unabhängig entwickelte Plattform MASH IoT ist ein Beispiel des Systems, welches das Management (Überwachung, Steuerung und Konfiguration) der IoT-Ressourcen erleichtern kann, und zwar überall und in Echtzeit, mittels eines IoT-Dashboards in Smartphones. Eine geeignete Verwaltung wird auch von der Einhaltung der Kompatibilität in allen IoT-Schichten zur Optimierung der Anschlussgeschwindigkeit und Sicherstellung der Dienstleistungserbringung gebraucht. Die Arbeitsgruppe fürs Management der Geräte im Rahmen der Allianz **OMA** (*Open Mobile Alliance*) erstellt Protokolle und Mechanismen fürs Management der mobilen Geräte und Dienste in ressourcenbeschränkten Umgebungen.

Fertigung

Die Herausforderungen im Bereich Fertigung müssen überzeugend gelöst werden. Die Kosten eines passiven RFID-Tags müssen unter einen Cent reduziert werden und die Produktion muss extrem große Mengen erreichen. Dabei muss der ganze Fertigungsprozess nur geringe Auswirkungen auf die Umwelt haben und auf Wiederverwendungs- und Abfallverwertungsstrategien in dem ganzen Lebenszyklus der digitalen Geräte und weiterer Produkte basieren, die etikettiert werden oder sensoraktiv sein.

5.2 Hindernisse

Es gibt jedoch auch Hindernisse fürs IoT, vor allem im Bereich der Regelung und Sicherheit. Das Hauptziel besteht im Schutz der Privatsphäre der Personen und Zwang der Firmen zur Einführung der sicheren Datenverwaltung [8, 9].

Absenz der Überwachung

Eines der größten Hindernisse der weitverbreiteten Einführung der IoT-Technologien ist die Absenz der Überwachung. Ohne ein unabhängiges Überwachungsorgan kann nie ein wirklich globales IoT entstehen, das von Staaten, Firmen, Handelsorganisationen und Öffentlichkeit akzeptiert wird. Heutzutage gibt es kein unikales und universales Nummerierungsschema: EPCglobal und Ubiquitous Networking Lab schlagen zwei unterschiedliche, nicht kompatible Verfahren zur Identifikation der Objekte vor und es droht die Gefahr, dass sie in den folgenden Jahren auf dem Weltmarkt konkurrieren werden. Weiter soll die Überwachung möglichst generisch gehalten werden, weil ein gesondertes Organ für jedes einzelne Feld sicher zum Überlappen und Verwechselung der Standards führen würde. Die Objekte können unterschiedliche Identitäten in unterschiedlichen Kontexten haben und daher könnte die Einführung von mehr Organen eine Art von Multi-Homing und nachfolgend sogar katastrophale Folgen verursachen.

Privatsphäre und Sicherheit

Für eine allgemeine Akzeptanz eines Identifikationssystems der Objekte muss eine technisch solide Lösung zur Sicherstellung der Privatsphäre und Sicherheit der Kunden vorgestellt werden. Weil die Sicherheit häufig als eine Zusatzeigenschaft ausgeführt wurde, herrscht die Meinung, dass das IoT von der Öffentlichkeit nur dann akzeptiert wird, wenn es eine robuste Lösung der Sicherheit und Privatsphäre hat. Vor allem müssen Angriffe abgefangen, Daten authentifiziert, Zugriffe kontrolliert und die Privatsphäre der Kunden (der natürlichen und juristischen Personen) gewährleistet werden. Dabei kann es sich um hybride Sicherheitsmechanismen handeln, die beispielsweise Hardwaresicherheit und Schlüsseldiversifizierung kombinieren, um eine ausgezeichnete Sicherheitsebene zu garantieren. Eine solche Sicherheit kann dann Angriffe erheblich erschweren oder sogar verhindern. Die Auswahl der Sicherheitsfunktionen und -mechanismen wird nach wie vor von ihrer Auswirkung auf die Geschäftsprozesse abhängen; immer werden Kompromisse zwischen der Größe, Kosten, Funktionalitäten, Interoperabilität, Sicherheit und Privatsphäre geschlossen.

In den künftigen Standards sollen die Fragen der Sicherheit und Privatsphäre gelöst und die einzelnen Sicherheitsfunktionen zur Unterstützung der Vertraulichkeit, Integrität oder Verfügbarkeit der Dienste definiert werden.

Es gibt auch viele Probleme hinsichtlich der Identität der Personen. Sie müssen im Rahmen der Regelung und Legislatur behandelt werden, weil sie für ein effektives Funktionieren der öffentlichen Verwaltung in der Zukunft von großer Bedeutung sind.

6 Zukunft des IoT

Für die nächsten Jahre können vier Makrotrends identifiziert werden, welche die Zukunft der Internettechnologien zusammen mit dem raschen Anstieg der ubiquitären IoT-Geräte prägen werden [9]:

1. Der erste Trend wird manchmal als „exaflood“ oder „Datenflut“ bezeichnet - es handelt sich um eine explosive Erhöhung der Anzahl von erfassten und ausgetauschten Daten. Weil die bestehenden Netzwerke für diese exponentielle Verkehrszunahme nicht vorbereitet sind, müssen alle Beteiligten die gegenwärtigen Architekturen der Netzwerke und Speicher neu gestalten. Es wird dringender denn je, dass neue Verfahren und Mechanismen für die Suche, Erfassung und Übertragung von Daten gefunden werden. Eine der Ursachen dieser Datenflut ist die extreme Zunahme der Anzahl der Geräte, welche Informationen sammeln und austauschen, wenn IoT zu einer Realität wird.

Der Begriff **exaflood**, der von Bret Swanson aus der Stiftung für Fortschritt und Freiheit (Progress & Freedom Foundation) erfunden wurde, bezeichnet die wachsende Menge von Daten im Internet.

2. Die für den Betrieb der intelligenten Geräte erforderliche Energie wird dramatisch sinken. Schon heutzutage haben viele Datenzentren ihr Maximum des Energieverbrauchs erreicht und daher wird die Ergänzung von neuen Geräten zwangsläufig mit dem Ausscheiden der alten bedingt. Daher kann hier der zweite Trend beobachtet werden, der alle Geräte und Systeme ab kleinsten smarten Komponenten bis riesigen Datenzentren betrifft: die Suche der Nullentropie oder anders gesagt des Zustandes, in dem das Gerät oder System seine eigene Energie ernten wird.

3. Miniaturisierung der Geräte erfolgt auch erstaunlich schnell. Das Ziel eines Transistors mit einem einzigen Elektron rückt immer näher - dies scheint als die unüberschreitbare Grenze, bis neue einschneidende Entdeckungen in Physik gemacht werden.

4. Der vierte wichtige Trend besteht in autonomen Ressourcen. Die ständig wachsende Komplexität der Systeme wird unüberschaubar und wird die Erzeugung neuer Dienste und Anwendungen verhindern, ohne dass die Systeme über eine viel größere Selbstständigkeit verfügen werden, wie Selbstverwaltung, -heilung und -konfigurierung.

Weil die Integration der Technologien in physische Objekte allgemein billiger wird, wird die Akzeptanz und Verwendung des IoT weiter steigen. Infolgedessen wird IoT erhebliche Auswirkungen sowohl auf Business-to-Business- als auch Business-to-Consumer-Firmen in den kommenden Jahren haben.