

Cloud Computing und das Internet der Dinge

Inhaltsverzeichnis

1 Cloud Computing und das Internet der Dinge	3
DOMINIK DESCHNER, PAUL STUWE	
1.1 Einleitung	3
1.1.1 Ziel der Arbeit & Gang der Untersuchung	4
1.2 Grundlagen	4
1.2.1 Internet der Dinge	4
1.2.2 Übersicht über den IoT-Markt	9
1.2.3 Schlüsseltechnologien des IoT	10
1.3 Quantitative Analyse ausgewählter IoT Cloud-Angebote	13
1.3.1 Auswahl der zu untersuchenden Cloud-Anbieter	13
1.3.2 Azure IoT Central	15
1.3.3 Amazon AWS IoT	18
1.3.4 Evaluation der vorgestellten Angebote	20
1.4 Herausforderungen der Nutzung von Cloud Computing im IoT-Umfeld	21
1.4.1 Sicherheit	21
1.4.2 Vendor Support	22
1.4.3 Geopolitische Spannungen	22
1.5 Fazit, Diskussion und Ausblick	23
Literatur	24

1 | Cloud Computing und das Internet der Dinge

DOMINIK DESCHNER, PAUL STUWE

1.1 Einleitung

„Industrie 4.0“ - nicht viel weniger als das Paradigma der vierten industriellen Revolution wird maßgeblich durch das Aufkommen von miteinander und mit dem Internet vernetzten Geräten aller Art - dem „Internet of Things“ in Verbindung gebracht bzw. beeinflusst [Sic23b]. Bezogen auf die nächsten fünf Jahre sind, gemäß einer Statista-Studie, jährliche Marktwachstumsraten von rund 16 Prozent zu erwarten, aktuell (2023) werden jährliche Umsätze in Billionenhöhe[sic] generiert[Sta23].

Die allgegenwärtige, in den vergangenen Jahren stetig fortschreitende Vernetzung von Gegenständen, Gebäuden oder auch dem öffentlichen Raum verändert den Alltag der Menschen und führt auf gesellschaftlicher und wirtschaftlicher Ebene zu Disruption. [Gla15] Die Ausdehnung des IoT hat bereits 2019 die des von Menschen geprägten Internets überholt [Sta22]. Die Potenziale und das Spektrum möglicher Anwendungsfälle sind enorm und reichen von „smarten“, vernetzten Hausgeräten im Consumer-Bereich bis hin zu voll vernetzten (Offshore-)Industrieanlagen, Parkleitsystemen oder ganzen Versorgungsnetzen, dem so genannten Smart Grid [Gla15]. So vielfältig wie die Anwendungsfälle des Internets der Dinge sind auch die jeweils (von Herstellern und Anwendern) verfolgten Ziele. So kann angenommen werden, dass z. B. im Kontext von Smart Home vor allem der Komfort und wahrgenommene Nutzen der Anwender im Vordergrund steht, wogegen im industriellen Internet der Dinge das Realisieren von Effizienzsteigerungen oder Optimieren von Wartungsintervallen und Ausfallzeiten im Fokus liegt.

Vor allem die Bereitstellung von Rechenleistung in der Cloud ist notwendige Voraussetzung, um mit leistungsfähigen IoT-Lösungen am Markt bestehen zu können. Cloud Computings ermöglicht Anwendern („cloud consumers“) eine einfache und insbesondere ökonomische (da flexibel und skalierbar) Nutzung von IT-Ressourcen. Entsprechende Servicemodelle von Cloud-Anbietern („provider“) decken hierbei eine Vielzahl von Bedarfen, von der reinen Infrastruktur bis hin zu vollständig fremd gehosteten Anwendungen, ab [Gra12]. Unternehmen können ihren Ressourceneinsatz so flexibler gestalten, was in der Folge ein agileres Agieren ermöglicht.

Die Bandbreite unterschiedlicher IoT-Lösungen und mit diesen realisierten Anwendungsfällen erfordert den Einsatz entsprechend unterschiedlicher Technologien und Systemarchitekturen. Besonderes Augenmerk kommt hierbei der sachgerechten Auswahl dieser Technologien und Architekturen zu, da diese entscheidend für den nachhaltigen Erfolg von IoT-Lösungen sind [Al-+15]. Cloud-Anbieter decken durch ihre flexiblen Angebote diese Bedarfe, z. B. durch die Vielfalt möglicher Programmiersprachen im Rahmen von Platform-as-a-Service-Angeboten, ab [Gra12].

1.1.1 Ziel der Arbeit & Gang der Untersuchung

Ziel dieser Arbeit ist es daher, die elementare Bedeutung von Cloud Computing als Schlüsselement leistungsfähiger IoT-Lösungen aufzuzeigen. Es wird zunächst ein Überblick über wichtige Konzepte des „Internets der Dinge“ gegeben und hierbei insbesondere für die Umsetzung von IoT-Lösungen erforderliche Schlüsseltechnologien aus dem Umfeld des Cloud Computings herausgestellt. Hierzu werden die einschlägigen, zum Verständnis dieser Arbeit notwendigen, begrifflichen Grundlagen und Meilensteine der Entwicklung erläutert. Darauf aufbauend werden sodann ausgewählte, gegenwärtig am Markt verfügbare Angebote von Cloud Computing-Diensten im Kontext des Internets der Dinge dargestellt und diese quantitativ anhand von Kennzahlen, die aktueller wissenschaftlicher Literatur entnommen sind, miteinander verglichen. Die Arbeit schließt mit der Diskussion gegenwärtiger Herausforderungen hinsichtlich der Nutzung des Internets der Dinge und gibt einen Ausblick auf mögliche künftige Entwicklungen, ebenfalls unter Bezugnahme auf die Rolle des Cloud Computings.

1.2 Grundlagen

Dieses Kapitel behandelt fachliche und begriffliche Grundlagen die zum tieferen Verständnis dieser Arbeit notwendig sind.

1.2.1 Internet der Dinge

Das Internet der Dinge (IoT) beschreibt eine Reihe an Technologien und Trends, die es ermöglichen, dass immer mehr Gegenstände mit Sensoren, Aktuatoren und Mikrocontrollern ausgestattet sind und über Netzwerkschnittstellen untereinander oder mit dem Internet kommunizieren können. Die daraus resultierende zunehmend ubiquitäre Digitalisierung von Gegenständen und Maschinen lässt digitale und reale Welten immer weiter miteinander verschmelzen und stellt das Fundament für eine Vielzahl neuartiger Anwendungsfälle. Mithilfe von Sensoren werden Dinge in die Lage versetzt, Zustände und Vorgänge ihrer Umwelt zu erfassen. Durch Aktuatoren können sie wiederum mit dieser interagieren. Über eine Netzwerkverbindung können Daten mit anderen smarten Geräten oder Cloud-Diensten ausgetauscht werden und so Entscheidungen autonom getroffen sowie komplexe Szenarien dezentral realisiert werden [Al-+15].

Abb. 1.1 zeigt, dass die Paradigmen und Technologien des Internets der Dinge in unterschiedlichen Bereichen Anwendung finden und dort in domänenspezifischen Lösungen integriert werden. Die Vielzahl und Heterogenität der von Al-Fuqaha u. a. aufgelisteten Anwendungsgebiete lässt Rückschlüsse auf die Diversität der unterschiedlichen IoT-Systeme schließen.



Abbildung 1.1: Anwendungsbereiche des Internets der Dinge [Al-+15]

So unterscheidet sich die Implementierung von IoT-Systemen in den beispielhaft gewählten Bereichen Smart Home und Industrie 4.0 grundsätzlich. Zwar werden in beiden Systemen Dinge miteinander vernetzt, jedoch werden jeweils verschiedene Messwerte erhoben und unterschiedliche Übertragungstechnologien oder Konzepte zur Datenverarbeitung, wie z. B. das an anderer Stelle in dieser Arbeit noch detaillierter dargestellte Edge Computing, eingesetzt. Dennoch lassen sich die IoT-Systeme aus beiden zuvor beschriebene Anwendungsbereichen mit dem in Abb. 1.2 skizzierten Architekturmodell, welches den Aufbau einer IoT-Lösung abstrakt zeigt, beschreiben [Tas21]. Daraus ergeben sich die im Folgenden erläuterten Architekturebenen:

Geräteschicht Auf dieser Ebene befinden sich die IoT-Geräte, welche Messgrößen aus ihrer Umwelt erfassen oder mittels Aktuatoren auf diese einwirken und fortlaufend Daten generieren. [Al-+15]

Netzwerkschicht In der Netzwerkschicht werden die Daten aus der Geräteschicht vorverarbeitet und aggregiert oder direkt an die Plattform-Schicht weitergeleitet. [Al-+15]

Plattform-Schicht Auf dieser Ebene werden die Daten vieler Geräte in einer Cloud-Lösung gespeichert und verarbeitet. Dabei können Informationen, wie zum Beispiel Steuersignale, an die Geräteschicht zurückübertragen werden. Ebenso findet hier die Aufbereitung für die Anwendungsschicht statt. [Al-+15]

Anwendungsschicht Auf der Anwendungsschicht werden Softwarelösungen für den Endanwender der Anwendung wie beispielsweise Dashboards oder Webanwendungen bereitgestellt. [Al-+15]

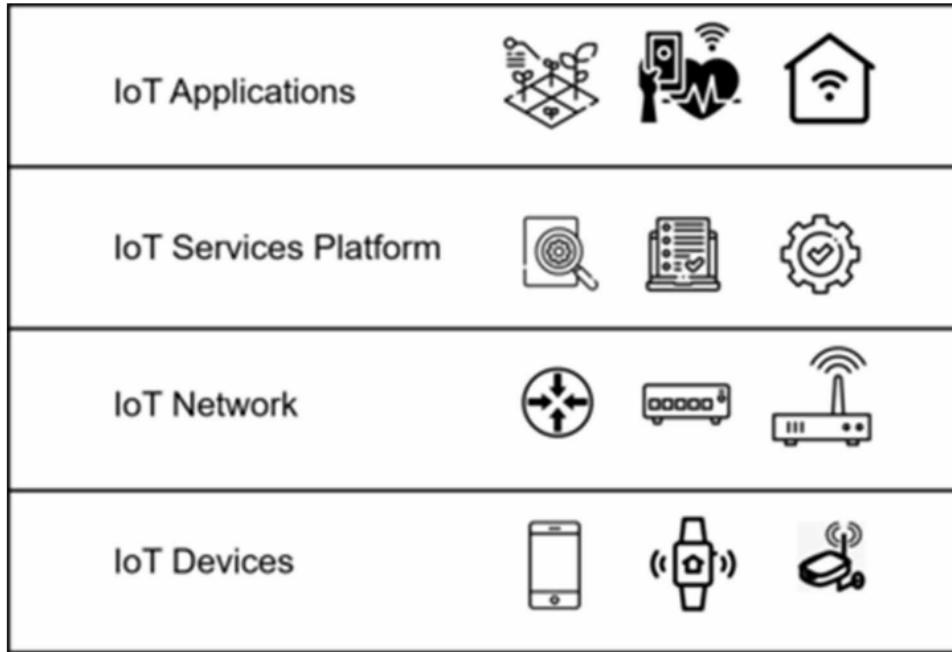


Abbildung 1.2: Architektur eines IoT-Systems [Tas21]

Entstehung & Prägung des Begriffs Internet der Dinge

Die Zuschreibung der Erfindung des Begriffs „Internet der Dinge“ erfolgt gemeinhin dem damaligen Mitarbeiter von Procter & Gamble, Ashton. Diesen Begriff verwendete dieser im Jahr 1999 im Kontext der Verbindung von Radio Frequency Identification (RFID)-Techniken und dem Internet. Es sei jedoch angemerkt, dass die genaue Entstehungsgeschichte nicht zweifelsfrei dokumentiert ist, da schriftliche Belege hierzu fehlen. In 2009 umreißt Ashton seine damalige Vision, die darauf abzielte, Computer im Internet der Dinge autonom in der Lage zu versetzen, Informationen aus ihrer Umwelt zu erfassen, ohne (ausschließlich) von menschlichen Eingaben abhängig zu sein [Ash09].

Die Idee von Ashton fand ab 2004 zunehmendes Interesse in der Forschung und wurde durch wesentliche Fortschritte in der Miniaturisierung und kosteneffizienten Fertigung von Sensoren und Mikrocontrollern, Ausbau der Mobilfunknetze und der Etablierung von Cloud Computing begünstigt [AIM10]. Gershenfeld, Krikorian und Cohen betonen die Vorteile von Geräten, die autonom über IP-Pakete miteinander kommunizieren können, und skizzieren ihre Vision anhand eines vernetzten Smart Homes [GKC04]. In ähnlichem Kontext betonte [Con06] die immense Bedeutung mobiler Datenübertragung für das Internet der Dinge. Atzori, Iera und Morabito geben einen umfangreichen Überblick über die relevanten Technologien im Internet der Dinge und gehen auf konkrete Anwendungsgebiete in beispielsweise der Logistik oder dem Gesundheitswesen ein.

Wie aus Abb. 1.3 hervorgeht, hat sich die anfängliche Idee der genannten Pioniere zu einem prominenten Forschungsgebiet entwickelt.

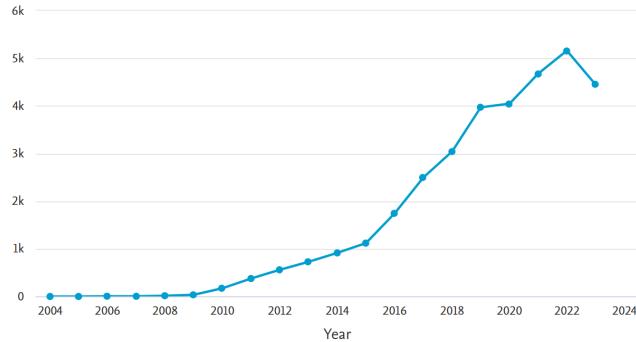


Abbildung 1.3: Scopus-Auswertung der Publikationen pro Jahr für folgende Abfrage: TITLE („internet of things“) AND PUBYEAR > 2003 AND PUBYEAR < 2024

IoT Value Stack

Zur detaillierteren Darstellung der Komponenten einer IoT-Lösung wurde im vergangenen Kapitel bereits ein *technisches* Architekturmodell vorgestellt. Zur Erläuterung, wie durch das Zusammenwirken verschiedener Ebenen die Wertschöpfung einer IoT-Lösung für den Kunden erzeugt wird - im Sinne einer *betriebswirtschaftlichen* Perspektive -, kann der „IoT Value Stack“ herangezogen werden. Dieser geht auf Fleisch et al. zurück und beschreibt, wie eine physische, lokale Ebene (Mikroprozessoren, Sensoren, Konnektivität, Software) mit einer digitalen, globalen Ebene (die den Nutzen der lokalen Ebene erweitert bzw. verbessert) zusammenwirkt und so ein hybrides Wertversprechen generiert. [FWW14]. Lösungen sind bedarfsgerecht skalierbar und stehen global zur Verfügung. [WF15]

Die Bedeutung von Cloud Computing-Technologien für die Wertschöpfung einer IoT-Lösung wird hier durch einen eigenen Layer verdeutlicht. In einer Cloud-Umgebung werden einerseits Daten aus dem Feld aggregiert, analysiert und an den Nutzer ausgeliefert bzw. dem Unternehmen für analytische Zwecke bereitgestellt, andererseits ermöglicht die Bereitstellung von IT-Infrastruktur in der Cloud herstellerseitig auch ein effektives Controlling von Dienstkosten einer Lösung.

Im Folgenden werden die Bestandteile des IoT Value Stack grafisch dargestellt Abb. 1.4 und anhand eines praktischen Beispiels aus dem Smart Home-Bereich („smarte Glühlampe“) näher erläutert.

Physischer Gegenstand: Dieser bildet die „Ausgangsbasis“ einer IoT-Lösung. Eine Glühbirne stiftet in ihrer unmittelbaren lokalen Umgebung einen Nutzen in Form von Licht und somit Sicherheit und Komfort. Im Hinblick auf die folgenden Schichten wird das physische Produkt um digitale Dienste und Funktionen erweitert. [FWW14; EW16; WF15]

Sensoren/Aktuatoren: Diese erlauben es dem Produkt, Informationen über seine Umwelt zu sammeln oder mit dieser zu interagieren. Im Falle der Glühbirne ist der Lampenkörper mit einem Bewegungssensor ausgestattet, der die An-/Abwesenheit von Personen in der Umgebung detektiert und das Licht bedarfsgerecht ein-/ausschaltet. Der lokal gestiftete Nutzen wird auf diese Weise bereits erweitert. [FWW14; EW16; WF15]

Konnektivität: Insbesondere drahtlose Kommunikation wie WLAN, Bluetooth oder NarrowBand IoT ermöglichen es, lokal mit anderen Gegenständen zu kommunizieren oder eine Verbindung zum Internet herzustellen. Die Glühbirne übermittelt über diese Schnittstelle ihren Betriebszustand, der sodann von berechtigten Anwendern von überall eingesehen werden kann. [FWW14; EW16; WF15] Das Aufkommen von 5G-Netzwerken und die hiermit verbundene gesteigerte

Bandbreite, niedrige Latenz und hohe Kapazität dieser Netzwerke begünstigt das Wachstum von IoT-Ökosystemen und ermöglicht Echtzeit-Interaktion mit IoT-Geräten [Sta23].

Analytics: Da Konnektivität allein den Nutzen eines Dinges noch nicht erweitert, ist eine Analytics-Ebene notwendige Bedingung. Hier tritt nun erstmals ein Cloud-Bezug in Erscheinung. Daten, die von den Gerätesensoren gesammelt wurden bzw. Daten, die an die Geräte ausgeliefert werden sollen, werden hier aggregiert, gespeichert, plausibilisiert und analytisch behandelt. Im Fall der Glühbirne wird die Analytics-Ebene verwendet, um aus einzelnen Daten zu Betriebszuständen eines Leuchtmittels Bewegungsmuster und übliche Betriebszeiten zu generieren. [FWW14; EW16; WF15]

(Digitaler) Service: Das nunmehr hybride Wertversprechen des physischen Gegenstands wird in digitale Services gekapselt (z. B. als Webservice oder Smartphone-App) und global zur Verfügung gestellt. Der Benutzer kann die Glühbirne nun nicht nur als lokale Lichtquelle, sondern z. B. als primitives Sicherheitssystem nutzen, mit welchem mögliche Einbrecher durch das gezielte Einschalten des Lichts abgewehrt werden können. [FWW14; EW16; WF15]

Erwähnenswert ist, dass die Kosten für den Betrieb einer solchen Lösung - insbesondere die Grenzkosten im Sinne der Erweiterung des Nutzendenkreises um eine weitere Person - bei IoT-Lösungen marginal sind. Zu beachten ist außerdem, dass IoT-Lösungen zumeist ganzheitlich entwickelt werden müssen, da nicht das bloße Hinzufügen der beschriebenen Schichten den hybriden Nutzen stiftet, sondern nur eine integrierte Entwicklung unter Berücksichtigung der digitalen Dienste der höheren Ebenen. [FWW14].

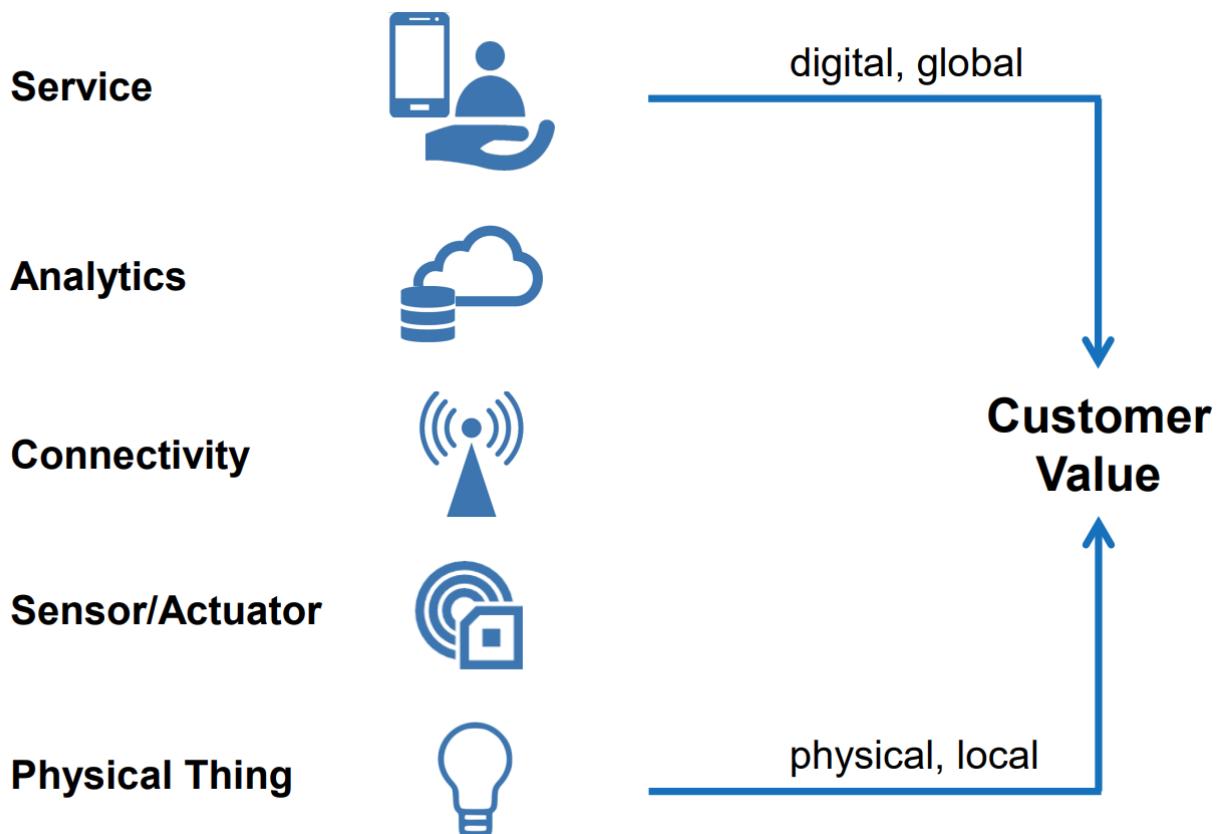


Abbildung 1.4: IoT-Value Stack Grafik nach [FWW14]

Aktuelle Entwicklungen im IoT-Umfeld

Wie bereits dargestellt, umfasst der Begriff des „Internets der Dinge“ eine Vielzahl an Konzepten und Betrachtungsperspektiven. Dies bedeutet gleichermaßen, dass das Themenfeld ebenfalls Trends und der Begriff einem Bedeutungswandel unterliegt. Gemäß einer aktuellen Statista-Studie werden gegenwärtig (Stand Herbst 2023) 5G-Mobilfunktechnologie, Sicherheitsaspekte des IoT, „Artificial Intelligence of Things (AIoT)“ sowie Edge Computing als Trends identifiziert [Sta23]. Diese Themen werden z. T. im weiteren Verlauf dieser Arbeit näher beschrieben.

1.2.2 Übersicht über den IoT-Markt

Wie in der Einleitung erwähnt, hat das Marktvolumen für IoT-Lösungen mittlerweile die Billionengrenze erreicht - Tendenz steigend. Die bereits erwähnte Statista-Studie identifiziert sieben Marktsegmente für IoT-Lösungen. Diese Ausarbeitung bzw. der folgende Abschnitt konzentriert sich auf die beiden Ausprägungen „Consumer IoT“ und „Industrial IoT“. Hierbei handelt es sich jeweils um das zweit- bzw. drittgrößte Marktsegment. Das größte Marktsegment stellt „Automotive IoT“ dar, wird im Rahmen dieser Arbeit jedoch nicht betrachtet.

Consumer IoT

Consumer IoT bezieht sich auf mit dem Internet verbundene Geräte (jedoch keine Personal Computer im Sinne von Notebooks, Tablets o. ä.), die von Verbrauchern im privaten (häuslichen) Umfeld verwendet werden. Eine bekannte Ausprägungsform sind Smart Home-Geräte oder (Fitness-)Wearables. Mit Stand 2023 werden rund 10 Milliarden Consumer IoT-Geräte betrieben, das Marktvolumen liegt bei rund 180 Mrd. US-\$. Es ist ein globales Wachstum zu beobachten, da Verbraucher flächendeckend ihr Zuhause und ihre tägliche Lebensführung um IoT-Technologien ergänzen, insbesondere in den USA und Deutschland. Marktführend im Umfeld Consumer IoT sind die Unternehmen Qualcomm (v. a. für Mikrochips und Software für Mobilfunkanwendungen) sowie Bosch. [Sta23]

Consumer IoT-Geräte zeichnet im Vergleich zu Geräten des unten beschriebenen Industrial IoT (IIoT) aus, dass sie i. d. R. Komfort für den Verbraucher bereitstellen, wohingegen IIoT-Anwendungen primär die Überwachung der Wertschöpfung zum Ziel haben [Sis+18]. Der Zugriff auf die „smartten“ Funktionalitäten erfolgt i. d. R. über „Companion Apps“, wenngleich eine steigende Popularität der Steuerung über Sprachassistenten wie Siri oder Alexa zu erkennen ist [Kom22]. Eine weitere Quelle stellt die Abgrenzung in Segmente wie CIoT bzw. IIoT infrage und benennt eine steigende Konvergenz der einzelnen Segmente, nimmt jedoch hinsichtlich CIoT/IIoT eine Abgrenzung in „Innen- bzw. Außenansicht“ vor - IIoT-Anwendungen dienen Unternehmen etwa der nach innen gerichteten Prozessoptimierung, wohingegen eine CIoT-Lösung ein Produkt und einen Service zur bereits beschriebenen Stiftung eines Nutzens bündelt. [Lew23]

Herausforderungen im Bereich Consumer IoT waren etwa Gegenstand einer 2022 veröffentlichten Untersuchung der Europäischen Union hinsichtlich des Wettbewerbs im IoT-Markt. Hierbei wurde die Interoperabilität zwischen Geräten verschiedener Hersteller als wichtige Challenge identifiziert, überdies eine Vereinheitlichung und Standardisierung einzelner Aspekte des Technologie-Stacks über „Basistechnologien“ wie WLAN oder Bluetooth hinaus, i. e. auf Betriebssystemebene. Aus Sicht des EU-Verbraucherschutzes ist auch die Vereinheitlichung heterogener Protokolle bzw. Standards betreffend den Datenaustausch und -schutz von Bedeutung sowie nicht zuletzt ein gleichberechtigter, performanter Zugang zu führenden Technologie-Plattformen. [Kom22]

Industrial IoT

Das Industrial Internet of Things umfasst die Anwendung von Technologien und Konzepten aus dem Bereich des Internets der Dinge im spezifischen Kontext industrieller Anwendungen. Im Gegensatz zum Consumer IoT, das tägliche Leben des Einzelnen komfortabler, einfacher und effizienter gestaltet, liegt beim IIoT der Fokus auf der Integration von Maschinen, Fertigungs- und Leitsystemen in die IT-Strukturen von Unternehmen. Der Zweck des IIoT besteht darin, die industrielle („smarte“) Produktion optimal zu steuern, Produktionsausfälle zu minimieren, Echtzeitüberwachung und die Fertigung von individualisierten Produkten zu ermöglichen. Dies wird erreicht, indem Maschinen und Systeme in Echtzeit miteinander kommunizieren und gleichzeitig nahtlos in die übergeordneten Geschäftsprozesse integriert werden. Effektive Vernetzung verschiedener Systeme, unabhängig von ihren Herstellern, ist entscheidend. In diesem Kontext spielt die Maschine-zu-Maschine-Kommunikation (M2M) eine essenzielle Rolle [Sis+18; XHL14].

Aus den zuvor beschriebene Zielen des IIoTs resultieren höhere Anforderungen hinsichtlich Latenz, Zuverlässigkeit, Reichweite und Sicherheit [Sis+18; XHL14].

Ökonomisch betrachtet beträgt das gegenwärtige Marktvolumen des IIoT-Marktes rund 280 Mrd. US-. Führende Unternehmen im Bereich IIoT sind General Electric (GE), Siemens, Schneider Electric und Bosch. [Sta23]

1.2.3 Schlüsseltechnologien des IoT

Zur Abrundung des Begriffsverständnisses und zwecks Einbezug aktueller Entwicklungen im Umfeld gibt dieser Abschnitt einen Überblick über wichtige Technologien, die i. d. R. Teil einer IoT-Lösung sind. Im folgenden Abschnitt erfolgt dann die quantitative Betrachtung wirtschaftlich bedeutender Cloud-IoT-Plattformen ohne konkreten Bezug zu einem „Thing“.

Big Data (Analytics) & Künstliche Intelligenz

Wie bereits der Value Stack zeigt, generiert die Nutzung einer IoT-Lösung zwangsläufig eine Reihe von Datenpunkten. Eine Quelle der EU konkretisiert dies - Daten werden durch Benutzereingaben, laufend bei der Verwendung oder automatisiert im Hintergrund erzeugt und können auch personenbezogen sein, sodass sie unter Normen wie die DSGVO fallen [Kom22]. Unternehmen wiederum sind in der Lage, Daten für ihre Wertschöpfung zu nutzen - wie North und Maier zeigen, hängt dies jedoch von der unternehmerischen Kompetenz zur Aneignung und Auswertung von Daten ab [NM18]. In der Regel werden die Daten auch den Anwendern zur Verfügung gestellt [Kom22]

Insbesondere bei einer Vielzahl von Geräten, die ein Hersteller in den Markt gebracht hat, können die hierbei entstehenden Daten u. U. (herstellerseitig) sogar als „Big Data“ klassifiziert werden. Dieser Begriff bezeichnet Daten, die aufgrund ihrer Größe „klassische“ Datenhaltung, Verarbeitung und Analyse auf konventioneller Hardware übersteigen [Fas16]. Eine Charakterisierung von Big Data kann anhand des 3V- bzw. 5V-Modells erfolgen:

Volume: Der Umfang der Daten umfasst mehrere Tera- bis Zettabyte. [Fas16]

Variety: Es werden strukturierte, semistrukturierte sowie unstrukturierte Daten gespeichert, zum Beispiel Datenbanktabellen, Dokumente, Grafiken, oder Audio/Video. [Fas16]

Velocity: Datenströme werden in Echtzeit analysiert bzw. ausgewertet. [Fas16]

Veracity: Daten sind von hoher Qualität und als korrekt anzusehen. [Fin18]

Value: Die zielgerichtete Verarbeitung von Daten verleiht ihnen einen (potenziellen) Wert. [Fin18]

Als Künstliche Intelligenz wird wiederum im Allgemeinen die Fähigkeit von Computern bezeichnet, menschliche kognitive Prozesse (unvollkommen) nachzubilden [Ert21]. So kann beispielsweise von „künstlicher Intelligenz“ bei Smart Home-Geräten gesprochen werden, die die Gewohnheiten ihrer Anwender im Laufe der Zeit selbstständig erlernen (z. B. An-/Abwesenheitszyklen bei Raumthermostaten) und automatische Anpassungen vornehmen [Mic24f] Insbesondere im Kontext aktueller Entwicklungen umfasst der Begriff vor allem Verfahren des maschinellen Lernens, das heißt die Bildung einer Regelbasis auf Basis von Trainingsdaten und mathematischer Verfahren und deren anschließende Anwendung auf unbekannte Eingabedaten [Kam20]. Eine Perspektive, die auf die deutsche Finanzaufsicht BaFin zurückgeht, verknüpft das Paradigma der Künstlichen Intelligenz mit „Big Data“ [Fin18]

Big Data und Künstliche Intelligenz („BDAI“) können als miteinander in Wechselwirkung stehend betrachtet werden, da aus Big Data nur dann ein (ökonomischer) Nutzen gezogen werden, wenn die Verarbeitung mittels KI-Verfahren erfolgt. KI-/ML-Verfahren sind wiederum auf eine hinreichend große Datenbasis zum Training des kognitiven Modells angewiesen. [Fin18]

Die Erfassung, Verarbeitung und Gewinnung von Erkenntnissen aus Big Data-Datasets mittels spezieller Tools und Systeme wird als „Big Data Analytics“ verstanden. Eine Definition von Microsoft benennt „intelligente Geräte“ als mögliche Quelle solcher Daten. Derartige Geräte generieren ein erhebliches Datenaufkommen, das es Unternehmen ermöglicht, Erkenntnisse zu gewinnen, Abläufe zu optimieren und künftige Entwicklungen vorherzusagen. Auch die schon durch den Value Stack angedeutete Symbiose mit Techniken des Cloud Computings wird hier benannt. [Mic24g]

Die Durchführung von Big Data Analytics erfolgt in einem mehrstufigen Verfahren, bei welchem Daten zunächst in einem Repository erfasst werden. Anschließend erfolgt eine Vorverarbeitung (Plausibilisierung, Sortierung, Filterung) sowie eine Bereinigung (Korrektur). Sodann werden die Daten über Methoden des maschinellen Lernens bzw. statistischer Verfahren analysiert, um Muster und Verhaltensweisen zu erkennen. Herausforderungen hierbei sind die Gewährleistung einer strukturierten Speicherung sowie der Datengovernance im Sinne von Verantwortlichkeiten und Qualitätsanforderungen [Mic24g].

Ein Trend in diesem Umfeld wird darüber hinaus als „Artificial Intelligence of Things“ (AIoT) bezeichnet. Die Integration von KI-Techniken in IoT-Lösungen verbessert die Effizienz, Profitabilität und die Entscheidungsfindungsfähigkeiten einer Lösung [Sta23]. Eine KPMG-Studie spricht hierbei von der Entwicklung zur „Community of Things“, bei der in IoT-Lösungen integrierte KI-Fähigkeiten sich mit Geräten in der Nähe verknüpfen, um gemeinsam Aufgaben durchzuführen [Wir18] Insbesondere die Anwendung maschineller Lernverfahren in Verbindung mit Daten, die von hoch entwickelten Sensoren generiert werden ermöglicht die Erkennung von Mustern und Anomalien, was vor allem in Anwendungsgebieten mit häufig veränderlichen Umweltbedingungen wie Luftverschmutzung, Temperatur, Feuchtigkeit oder Lärm bedeutend ist. 2022 wurde in 80 Prozent aller industriellen IoT-Vorhaben auch künstliche Intelligenz eingesetzt, da die Nutzung und primär die so ermöglichte Echtzeit-Analyse von Daten einen Wettbewerbsvorteil generiert [Sta23].

Edge Computing

Die fortschreitende Verbreitung des Internet of Things, sowohl im Endverbrauchersektor als auch in der Industrie, führt dazu, dass immer mehr Daten „am unteren Ende“ des Netzwerks, direkt an

den physischen Geräten, generiert werden. Obwohl die in den Cloud-Rechenzentren verfügbare Rechenleistung mit der enorm gewachsenen Datenmenge Schritt halten kann, stellt die begrenzte Bandbreite für die Datenübertragung in die Cloud einen limitierenden Faktor dar. [Shi+16]

Diese Herausforderung hat zur Entwicklung des „Edge Computing“ geführt, einer Technologie, die darauf abzielt, die Verarbeitung von Daten näher an der Quelle, also an den IoT-Geräten selbst, zu ermöglichen. Durch die Dezentralisierung der Rechenleistung können Engpässe bei der Übertragung von Daten in die Cloud verringert und Latenzzeiten minimiert werden. Dies bedeutet, dass bestimmte Daten direkt vor Ort verarbeitet werden können, ohne den Umweg über entfernte Rechenzentren nehmen zu müssen. Somit können ausschließlich relevante und aggregierte Daten zur Cloud übermittelt werden. Im Kontext von Wearable-Geräten fungiert das gekoppelte Smartphone als Edge-Komponente; im Bereich von Smart Home Anwendungen wird diese Aufgabe von einem sog. Gateway übernommen. [Shi+16]

Edge Computing bietet somit nicht nur eine effizientere Nutzung von Ressourcen, sondern auch eine schnellere Reaktionszeit, was in vielen Anwendungsgebieten von entscheidender Bedeutung ist. Diese Entwicklung trägt dazu bei, die Leistungsfähigkeit und Effizienz des gesamten Netzwerks einer IoT-Anwendung zu verbessern und ist somit ein wichtiger Baustein für skalierbare und flexible Architekturen. [Sat17]

Darüber hinaus spielt Edge Computing eine entscheidende Rolle im Kontext des Datenschutzes. Die Verlagerung von Rechenleistung näher an die Datenquelle reduziert die Notwendigkeit, sensible Informationen in die Cloud zu übertragen. Dies ist von besonderer Bedeutung, da viele IoT-Geräte persönliche oder geschäftskritische Daten generieren und trägt somit dazu bei, potenzielle Sicherheitsrisiken und Datenschutzbedenken zu minimieren, die mit der Übertragung sensibler Informationen über das gesamte Netzwerk verbunden sind. [SD16]

Ein weiterer bedeutender Vorteil von Edge Computing liegt in der Fähigkeit, die Kompatibilität und Flexibilität auf heterogener Gerätenebene zu verbessern. In IoT-Umgebungen kommen verschiedenste Gerätetypen und -hersteller zum Einsatz, was zu Komplikationen bei der Integration und Interoperabilität führen kann. Edge Computing ermöglicht eine dezentrale Datenverarbeitung, die auf unterschiedlichen Geräten und Plattformen stattfinden kann, ohne auf eine einheitliche Cloud-Infrastruktur angewiesen zu sein. [Mis22]

Beispielsweise bietet sich Edge Computing bei der Video- und Bildanalyse in Bezug auf die Qualitätssicherung in der Fertigung an. Würde der kontinuierliche Zufluss an Bildmaterial direkt in die Cloud übertragen werden und dort analysiert, so wäre die verfügbare Bandbreite schnell ausgereizt. Mithilfe von Edge Computing findet die Analyse vor Ort statt und lediglich Ergebnisse oder Ausreißer werden sporadisch in die Cloud übertragen. [Shi+16]

Auch die bereits genannte Marktanalyse von Statista benennt Edge Computing als wichtigen Enabler für Anwendungsfälle im Bereich „Smart City“ oder dem autonomen Fahren. [Sta23]

Digitale Zwillinge

Das Konzept der digitalen Zwillinge verweist auf die virtuelle und bidirektionale synchronisierte Repräsentation eines physischen Objekts im digitalen Raum. Dies bedeutet, dass physische Veränderungen an einem Objekt, wie beispielsweise einer Maschine, akkurat im digitalen Zwilling widergespiegelt werden. Gleichzeitig werden auch Anpassungen am digitalen Zwilling, etwa in Bezug auf Konfigurationen, vom physischen Objekt übernommen. [Ful+20]

Fundamental für dieses Konzept ist ein detailliertes Modell des physischen Gegenstands, welches Eigenschaften, Funktionen und Relationen umfassend in den Daten beschreibt. Digitale Zwillinge

können daher gezielt zur Vorhersage potenzieller Fehlerzustände oder Ausfälle herangezogen werden. Ein Aspekt, der hierbei an Bedeutung gewinnt, ist die Integration des IoT als Fundament für digitale Zwillinge. [Tao+19]

Das IoT fungiert dabei als Treiber für die Erfassung und Übertragung von Echtzeitdaten und Konfigurationsänderungen, welche die Grundlage für die Aktualisierung der digitalen Zwillinge bilden. Sensoren und intelligente Geräte im physischen Objekt ermöglichen eine kontinuierliche Daten erfassung, die unmittelbar in das digitale Modell einfließt. Diese enge Verknüpfung zwischen dem IoT und digitalen Zwillingen eröffnet neue Dimensionen der Echtzeitüberwachung, Analyse und Optimierung von realen Objekten. [Ful+20]

Heutige - praktische - Anwendungen für digitale Zwillinge liegen in der Verbesserung von Produktionsabläufen durch die Verbindung eines digitalen Zwilling mit VR und der Simulation von Ereignissen, die Validierung eines neuen Toolings vor dessen physischer Installation oder die Verbesserung der Fertigkeiten der Mitarbeitenden, um die Arbeitssicherheit und Handlungsfähigkeit des Personals zu steigern [Mic22c]

Die Verbindung von IoT und digitalen Zwillingen führt somit nicht nur zu Effizienzsteigerungen, sondern befähigt auch präventive Maßnahmen zur Fehlerbehebung und Optimierung von Systemleistungen in unterschiedlichen Anwendungsgebieten. Diese Konvergenz von Technologien ist insbesondere in verschiedenen Bereichen von Bedeutung, wie zum Beispiel in Smart Cities, dem Gesundheitswesen und der Industrie. [Ful+20] Wie eine von Microsoft und Intel durchgeführte Studie jedoch zeigt, sind Unternehmen bei der Implementierung digitaler Zwillinge mit großen Herausforderungen konfrontiert. Rund drei Viertel der Befragten nennen, neben allgemeinen Hindernissen wie Kosten oder Fähigkeiten des Personals, Schwierigkeiten bei der Integration, unzureichende Geschwindigkeit bei der Erstellung des digitalen Zwilling oder eine hohe Komplexität des Gesamt systems [Mic22c].

1.3 Quantitative Analyse ausgewählter IoT Cloud-Angebote

Nachdem im vorherigen Kapitel für das Verständnis der Untersuchung wichtige Begrifflichkeiten und Konzepte erläutert wurden, bildet dieses Kapitel nun den Hauptteil der Untersuchung. Da auch (bedeutende) Cloud-Anbieter („Hyperscaler“) das beschriebene Potenzial von IoT-Lösungen erkannt haben, bieten sie für Hersteller von IoT-Lösungen speziell zugeschnittene Produkte an. Diese ermöglichen es beispielsweise, die u. U. hohe Anzahl von Geräten einer IoT-Lösung in der Fläche optimal zu skalieren und auch unter Sicherheits-Gesichtspunkten zu betreiben [Mic24b]. Zur vertieften Untersuchung der Angebotsvielfalt werden aus einer aktuellen Marktanalyse eines renommierten Marktforschungsunternehmens in Verbindung mit aktueller Literatur verschiedene Angebote gewählt und diese im Hinblick auf Indikatoren und Kennzahlen, die sich ebenfalls aus der Literatur ergeben, verglichen. Ziel ist es, ein (dem jeweiligen Anwendungszweck angemessenes, siehe die Vielfalt von IoT-Lösungen) „optimales“ Angebot zu identifizieren.

1.3.1 Auswahl der zu untersuchenden Cloud-Anbieter

Im Folgenden wird das Vorgehen zur Auswahl der detailliert betrachteten Lösungen näher erläutert. Die im vorherigen Abschnitt referenzierte Marktanalyse wurde durch das Marktforschungsunternehmen Gartner entwickelt und zuletzt im Dezember 2022 veröffentlicht [Goo22]. Sie fokussiert sich primär auf Industrial IoT-Angebote; die in dieser Arbeit benannten „Cloud-Lösungen“ werden hier

als „IoT Platforms“ verstanden. Der Funktionsumfang dieser Lösungen erstreckt sich gemäß Gartner von der Geräteverwaltung einer IoT-„Flotte“, der Integration von Daten und Prozessen, dem Management und der (analytischen) Behandlung von Daten bis hin zu der Gewährleistung von Datenschutz und -sicherheit. In Abhängigkeit des Erfüllungsgrads der Dimensionen „completeness of vision“ und „ability to execute“ werden Anbieter in vier Quadranten eingeteilt, deren nähere Erläuterung jedoch den Rahmen dieser Arbeit übersteigt.

Muhammed und Ucuz bewerten in einer vergleichsweise aktuellen Studie die Cloud-Angebote der Unternehmen Microsoft, Amazon sowie Google. Deren Dienste werden anhand der Kriterien **Pricing**, **Verfügbarkeit**, **Vertraulichkeit**, **Abstufung des Leistungsumfangs (Tier Accounts)** sowie **Service Level-Vereinbarungen** evaluiert. Die Angebote von Microsoft, Amazon und Google werden hierbei als führend identifiziert; AWS erhält unter Sicherheits-, Analytics- und Schnittstellengesichtspunkten die beste Bewertung [MU20]. Kaushik u. a. beziehen in einen ähnlich gelagerten Vergleich das Pricing einzelner Anbieter (Microsoft, Amazon und Google) detaillierter ein und nehmen ergänzend einen Performance-Vergleich vor. Während Amazon das preiswerteste Angebot bereitstellt, bietet Microsoft im Allgemeinen die beste Performance bei gleichzeitig guter UX, wenngleich Amazon als führend bei den Einstellungsmöglichkeiten benannt wird. [Kau+21]

Ein Fachartikel von Microsoft benennt ergänzend wesentliche (hersteller-agnostische) Anhaltspunkte für die Auswahl eines Cloud-Anbieters, wenngleich diese Auswahl nicht auf IoT-Plattformen beschränkt ist [Mic24e]. Die Kriterien gliedern sich in die folgenden Dimensionen:

Wirtschaftliche Stabilität und Geschäftsprozesse: stabile finanzielle Situation, etablierte Kompetenzen in den Bereichen Organisation, Governance, Planung und Risikomanagement, kundenseitiges Vertrauen, technisches Know-How und Branchenwissen sowie der Nachweis der Erfüllung aller relevanten Anforderungen

Administrativer Support: Service Level-Vereinbarungen, Performance-Reports, Ressourcenüberwachung, Umsetzung eines Configuration Management-Prozesses, automatisiertes Accounting

Technische Funktionen und Prozesse: „einfache“ Bereitstellung und Verwaltung von Diensten, standardisierte Schnittstellen, Ereignis-Monitoring, Umsetzung eines Change-Management-Prozesses sowie die Unterstützung hybrider Betriebsmodelle

Sicherheitsmaßnahmen: Vorhandensein einer Sicherheitsinfrastruktur und -Richtlinien, Identity Management, Backup-Verfahren, physische Sicherheitsmaßnahmen

Grünberg und Schenck, welche die Cloud-Nutzung im IoT-Umfeld als „obvious approach“ für die Integration und Verarbeitung der gesammelten Daten benennen, betonen die **Performance** von Cloud-Plattformen als wichtigstes Kriterium zur optimalen Nutzung dieser Plattformen, insbesondere vor dem Hintergrund künftiger Echtzeit-Industrieanwendungen. In der durchgeföhrten Untersuchung wurde die Performance im Sinne hoher Verfügbarkeit und Leistung sowie niedriger Latenz definiert. Weitere wichtige Indikatoren sind laut Aussage der Autoren Skalierbarkeit, Kosten, das Abfangen von Lastspitzen sowie Fehlertoleranz. [GS18] Ray evaluiert in seinem Beitrag 26 Plattformen in diversen Anwendungsdomänen. Wichtige weitere Handlungsfelder bzw. Kennzahlen zur Leistungsmessung aus seiner Sicht sind u. a. der **Umgang mit heterogenen Daten**, die **Fähigkeit zur Standardisierung von Daten** sowie die **Adressierung einer erheblichen Anzahl von IoT-Endpunkten** (Node Identity) [Ray16].

Aus der vorliegenden Literatur - wenngleich aufgrund des beschränkten Umfangs dieser Ausarbeitung keine systematische Literaturrecherche durchgeführt werden konnte und die Ergebnisse daher

u. U. nicht vollständig den Stand der Forschung widerspiegeln, ergeben sich die IoT-Lösungen von Microsoft, Amazon und Google als sinnvoll vertiefend zu betrachtende Untersuchungsgegenstände. Microsofts im Folgenden dargestellte Lösung „Azure IoT Central“ wurde durch Gartner im Rahmen der Marktanalyse im „Leader“-Quadrant (hohe Erfüllung beider Dimensionen) verortet. Amazons Lösung, die „AWS IoT“-Dienstefamilie, ist im „Challenger“-Quadrant zu verorten, d. h. die „ability to execute“ ist ebenso hoch wie bei Microsoft, die „completeness of vision“ bleibt jedoch hinter Microsoft zurück [Goo22].

Eine vertiefte Untersuchung der in der Literatur identifizierten Lösung von Google, IoT Core, konnte im Rahmen dieser Ausarbeitung nicht sinnvoll erfolgen, da der Dienst zwischenzeitlich abgeschaltet wurde [Goo23]. Die generelle Implikation derartiger Entwicklungen wird im Verlauf dieser Arbeit nochmals im Kapitel „Herausforderungen“ aufgegriffen. Die nachfolgenden Unterabschnitte behandeln daher zunächst den Funktionsumfang der Angebote von Microsoft und Amazon, bevor sodann der Vergleich der Angebote anhand ausgewählter Kennzahlen erfolgt.

1.3.2 Azure IoT Central

Auf der Azure Cloud-Computing-Plattform stellt der Hyperscaler Microsoft unterschiedliche Dienste und Komponenten zur Realisierung von IoT-Anwendungen bereit. Die Cloud-Dienste sind modular aufgebaut, lassen sich untereinander verknüpfen und ergänzen sich in Bezug auf deren Funktionalität [Mic24a]. So kann beispielsweise der Azure IoT Hub, ein Dienst der die Verwaltung und Kommunikation zwischen IoT-Geräten und der Cloud ermöglicht, mit dem Azure Device Provisioning Service verbunden werden und so auf fortgeschrittene Load Balancing Mechanismen und Zuweisungslogik zurückgreifen [Mic23f]. Hierbei handelt es vorrangig um PaaS-Dienste, die durch den Anwender orchestriert und in seiner eigenen Softwarelösung integriert werden können. Azure IoT Central ist hierzu konträr als schlüsselfertige IoT Plattform positioniert und wird von Microsoft als application Plattform as a Service (aPaaS) bezeichnet [Mic23k]. Wie in Abb. 1.5 dargestellt ist Azure IoT Central mithilfe von anderen Azure Diensten aus dem IoT-Bereich umgesetzt. Dementsprechend eignet sich IoT Central gut, um einen Überblick über das Leistungsspektrum der grundlegenden IoT-Dienste von Azure zu erlangen. In den folgenden Abschnitten wird der Funktionsumfang von IoT Central und die korrespondierenden Azure-Dienste näher erläutert.

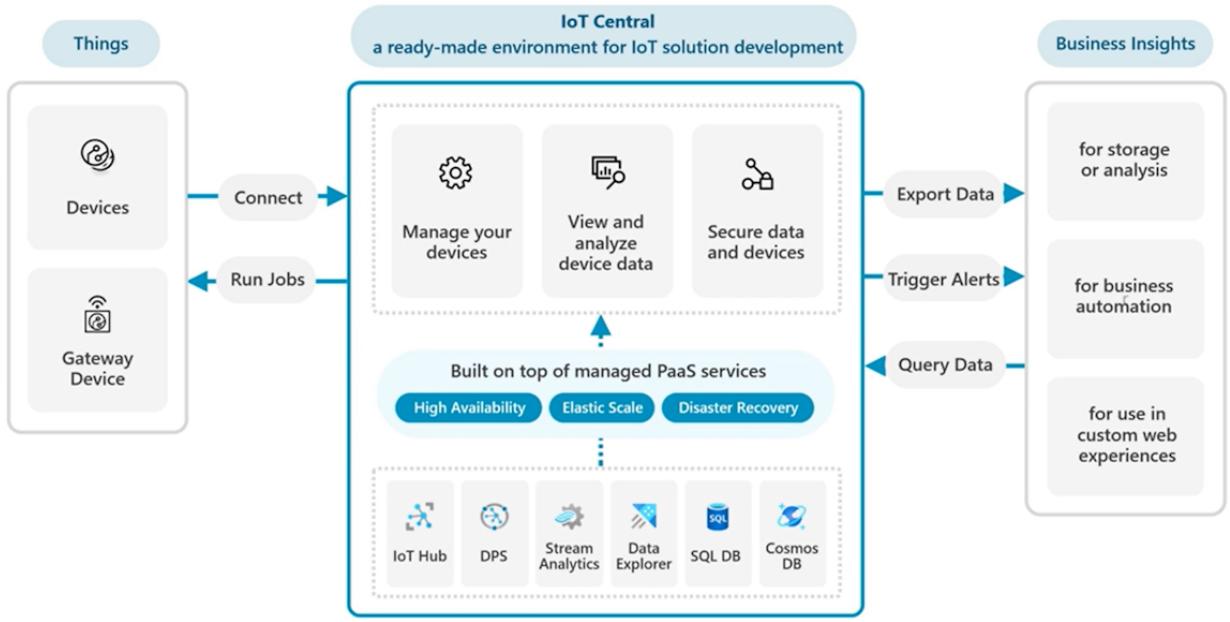


Abbildung 1.5: Service-Architektur von Azure IoT Central [Mic23a]

Allgemeine Funktionsbeschreibung

IoT Central ist eine kundenindividuell konfigurierbare IoT-Cloud-Platform zur Verwaltung, Übertragung und Verarbeitung von IoT-Daten in der Azure Cloud. Über das Azure Portal kann der Anwender eine oder mehrere Instanzen von IoT Central erstellen und unter einem eigenständigen DNS-Eintrag erreichen. In dem so erreichbaren Webportal kann der Anwender zunächst definieren, welche Datenstrukturen von den später eingesetzten IoT-Geräten übertragen werden oder welche Cloud-to-device-Operationen von diesen unterstützt werden. Im Anschluss können konkrete Geräte erstellt und über die von IoT Central bereitgestellten Verbindungszeichenfolgen angeschlossen werden. Mithilfe des von IoT Central bereitgestellten Gerätemanagements können die verbundenen IoT Geräte verwaltet, gerätespezifische Einstellungen vorgenommen und übertragene Messwerte und Betriebsdaten eingesehen werden. Weiterhin kann der Anwender Dashboards zur Aggregation und Visualisierung der IoT-Daten erstellen und Schwellwerte definieren bei deren Überschreitung der Anwender informiert wird. [Mic23k; Sta19]

Azure IoT Central stellt folglich grundlegende und generische Funktionen einer IoT-Cloud-Lösung bereit, die sich an die spezifischen Anforderungen verschiedener IoT-Szenarien anpassen lassen. Dafür muss der Anwender selbst keine Software auf der Anwendungsebene im Sinne des IoT Value Stacks entwickeln oder betreiben. Lediglich die Bereitstellung und Anbindung der IoT-Geräte an eine der unterschiedlichen Geräteschnittstellen von IoT Central liegen im Verantwortungsbereich des Anwenders. Entsprechend lassen sich eine Vielzahl verschiedener IoT-Szenarien mit IoT Central umsetzen, z. B. Überwachung und Fernwartung von Zapfsäulen [Mic21], Überwachung und Auswertung von Industriesteuerungen [Mic22b] oder Condition Monitoring in Lagerräumen [Mic20].

IoT Hub

Der Azure IoT Hub ermöglicht die Anbindung von IoT-Geräten an die Azure Cloud. Hierfür werden gängige Übertragungsprotokolle wie MQTT, AMQP oder HTTPS und verschiedene Authentifizierungsmechanismen wie X509-Zertifikate, SAS-Tokens oder Trusted Platform Module unterstützt [Mic18]. Über den IoT Hub können Nachrichten zwischen Cloud-Anwendungen und IoT-Geräten bidirektional ausgetauscht werden.

Um die hohen Anforderungen hinsichtlich eines flexibel und zielgerichteten Nachrichtenflusses innerhalb einer IoT-Lösung gerecht zu werden, unterstützt der IoT Hub unterschiedliche Kommunikationskonzepte.

Telemetrie-Nachrichten: Dienen der Übertragung von Datenpaketen, wie z. B. Sensormesswerten von IoT-Geräten an den IoT Hub. Eingehende Telemetrie-Nachrichten können vom IoT-Hub direkt an Cloud-Anwendungen weitergeleitet werden oder in Datenbanken bzw. Warteschlangen zwischengespeichert werden. [Sta19; Mic24c].

Cloud-To-Device-Nachrichten: C2D-Nachrichten ermöglichen die unidirektionale Übertragung von Cloud-Anwendungen an ein einzelnes Gerät, zum Beispiel zur Benachrichtigung über eine Zustandsänderung. Falls das adressierte Gerät beim Absenden der Nachricht nicht erreichbar ist, wird diese vom IoT Hub 48 Stunden gespeichert und zugestellt, wenn das Gerät wieder erreichbar ist. [Sta19; Mic23e]

Direkte Methoden: werden durch die Cloud-Anwendung initiiert und bedingen, dass das adressierte Gerät erreichbar ist und ad hoc den Eingang des Methodenaufrufs bestätigt. Das Gerät kann direkt auf den Methodenaufruf antworten und einen Rückgabewert an die Cloud-Anwendung übertragen. [Sta19; Mic23d]

Gerätezwilling: Die vom IoT Hub umgesetzten Gerätezwillinge orientieren sich am Konzept des Abschnitt 1.2.3. Pro Gerät wird vom IoT Hub ein dedizierter Gerätezwilling angelegt, welcher aus zwei relevanten Datenbereichen, den sog. „Reported Properties“ und den „Desired Properties“, besteht. Die „Reported Properties“ können nur von dem Gerät erstellt und geändert werden, die Cloud-Anwendung kann diesen Bereich lesen und über Änderungen informiert werden. Der Bereich „Desired Properties“ verhält sich hierzu konträr und kann von der Cloud-Anwendung beschrieben und vom Gerät gelesen werden. [Sta19; Mic23c]

Der IoT Hub bildet als zentrales, integrierendes Element das Fundament der Azure IoT-Dienste, da dieser Kommunikationsdienste für IoT-Anwendungen bereitstellt und so die Anbindung und Orchestration weiterer Dienste aus dem Azure-Portfolio ermöglicht.

Device Provisioning Service

In überregionalen oder globalen IoT-Szenarien kann es sinnvoll sein, mehrere IoT Hubs an verschiedenen geografischen Standorten zu betreiben, um Last zu verteilen und optimale Latenz sowie Bandbreite zu gewährleisten. Dies kann mit dem Device Provisioning Service realisiert werden, welcher mit einem oder mehreren IoT Hubs verknüpft werden kann und verschiedene Strategien zur Authentifizierung und Verteilung von IoT-Geräten bereitstellt. Mithilfe des Device Provisioning Service lässt sich sicherstellen, dass nach einer Standortänderung des Gerätes automatisch ein Transfer zu einem nahegelegenen IoT Hub stattfindet. [Mic23g; Sta19]

IoT Central verwendet den Device Provisioning Service, um die Registrierung neuer IoT-Geräte flexibel zu gestalten und von einzelnen IoT Hub-Endpunkten zu abstrahieren. Weiterhin wird die Offline-Registrierung via X509-Zertifikaten mit dem Device Provisioning Service realisiert.

Stream Analytics

In größeren IoT-Szenarien, welche eine Vielzahl von Geräten oder Messgrößen einschließen, müssen fortlaufend große, in der Cloud eingehende, Datenmengen erfasst und verarbeitet werden. Diese Anforderung kann in Azure durch den Stream Analytics Dienst erfüllt werden, welcher in der Lage ist, Datenströme aus mehreren Quellen zusammenzuführen, zu filtern, zu aggregieren und weiterzu-leiten. Hierfür können unterschiedliche Datenquellen mit dem Stream Analytics Dienst verknüpft werden, wie beispielsweise ein IoT Hub oder eine Datenbank. Über SQL-Abfragen wird definiert, welche Transformationen von der Stream Analytics Instanz vorgenommen werden. [Mic23j]

Stream Analytics eignet sich entsprechend zur Vorverarbeitung der eingehenden IoT-Daten, bevor diese längerfristig gespeichert werden. So kann zum Beispiel die gespeicherte Datenmenge durch zeitliche Aggregation reduziert werden. Jedoch kann auch komplexere Logik, wie zum Beispiel die Überprüfung von Grenzwertüberschreitungen, via Stream Analytics ausgeführt werden. [Mic23j] Die Skalierung der bereitgestellten Rechenleistung kann in Abhängigkeit zur eingehenden Datenmenge vorgenommen werden. So können Lastspitzen oder ungleichmäßige Datenströme, ohne au-ßerordentliche Verzögerung oder Überlastverhalten, verarbeitet werden [Mic22a].

1.3.3 Amazon AWS IoT

AWS (Amazon Web Services) IoT stellt das Leistungsangebot für IoT-Lösungen seitens des Hyperscalers Amazon dar. Mit dem Dienst ist es möglich, IoT-Geräte sowohl mit anderen Geräten als auch mit weiteren AWS-Clouddiensten zu verbinden. Es ist möglich, auf den jeweiligen Anwendungs-fall zugeschnittene Lösungen aus einer Vielzahl von Diensten zu kombinieren. Die Fähigkeiten der IoT-Plattform kann durch Dienste erweitert werden, die über das AWS IoT-Portfolio hinausgehen, z. B. für die Verwaltung von Daten, die Anwendung von KI oder zur Gewährleistung von Sicherheit. Beispiele hierfür sind Amazon Monitron für Machine Learning-Anwendungen oder AWS Panorama für Computer Vision [Goo22]. Wie die folgende Abbildung zeigt, stellt die Komponente „IoT Core“ die Schnittstelle zwischen Geräten und Clouddiensten dar.

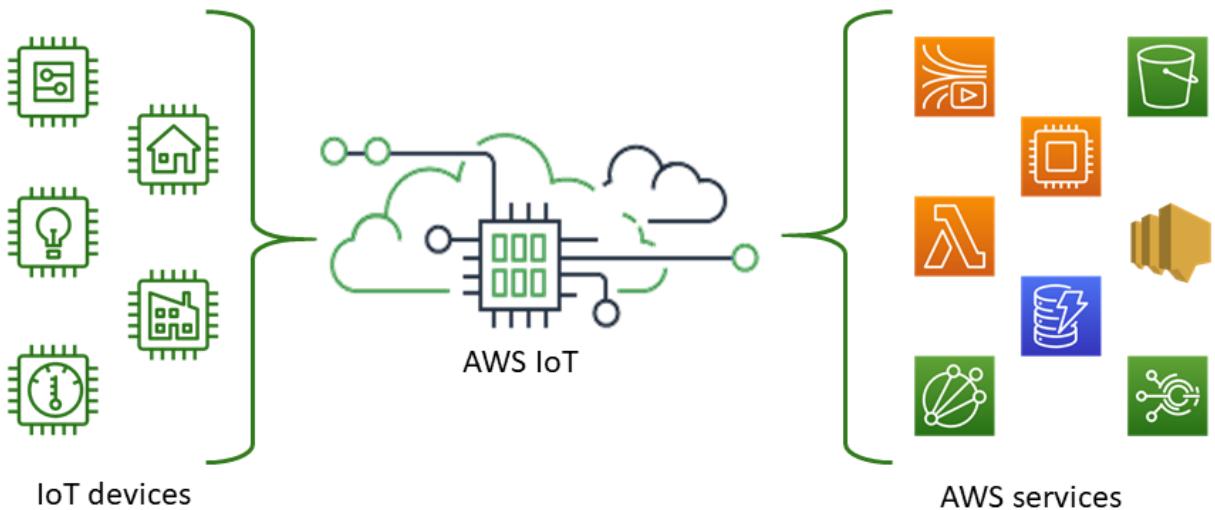


Abbildung 1.6: Service-Architektur von AWS IoT Hub [Ser23d]

Allgemeine Funktionsbeschreibung

AWS IoT stellt eine Reihe von Diensten zum Betrieb von IoT-Lösungen bereit. Der Umfang der angebotenen IoT-spezifischen Dienste wird durch Amazon in die drei Kategorien „Gerätesoftware“, „Konnektivitäts und Kontrolldienste“ sowie „Analytics“ untergliedert. [Ser23c]. Insgesamt besteht eine IoT-Cloudlösung laut „Developer Guide“ von Amazon aus einem Dienst zur Abwicklung der Verbindung und Verwaltung von IoT-Geräten, „compute services“ sowie Diensten zur Datenhaltung. [Ser23b]

Im Folgenden werden ausgewählte Dienste aus dem AWS IoT-Portfolio näher dargestellt.

AWS IoT Core

AWS IoT Core beinhaltet Funktionalitäten, um IoT-Geräte mit anderen IoT-Geräten sowie AWS-Clouddiensten verbinden. IoT Core fungiert hierbei als skalierbarer „Message Broker“, d. h. als Vermittler zwischen Geräten und AWS-Endpunkten [Ser23b]. Unterstützt wird eine Reihe verbereiteter, aktueller Protokolle wie MQTT, MQTT over WSS, HTTPS oder LoRaWAN (letzteres ist insbesondere im Kontext Smart City relevant) [Ser23d]. Eine vertiefte Erläuterung einzelner Protokolle würde jedoch den Rahmen dieser Arbeit übersteigen.

AWS IoT Greengrass

Bei AWS IoT Greengrass handelt es sich um einen Dienst, der dafür verwendet wird, IoT-Geräte mit Edge Computing-Fähigkeiten auszustatten. Mit Greengrass ist es möglich, von einem Gerät generierte Daten vorzuverarbeiten, ML-basierte Voraussagen zu treffen und Daten zu filtern bzw. zu aggregieren. Es ermöglicht zudem, dass Geräte auf lokale Ereignisse autonom reagieren und Daten mit Geräten im lokalen Netzwerk austauschen. Dies verringert insgesamt Kosten, da Daten nicht fortlaufend an die AWS-Cloud übertragen werden müssen [Ser23a] entsprechende Anwendungen können aus vorbereiteten Modulen zusammengestellt werden. [Ser23b]

AWS IoT Device Defender

AWS IoT Device Defender ist eine Lösung zum Schutz einer IoT-Geräteflotte. Konfigurationsparameter der Geräte werden fortlaufend überwacht und mit Best Practices abgeglichen. Im Falle einer Abweichung, z. B. bei der Nutzung von Identity Certificates über mehrere Geräte hinweg oder bei Verbindungsversuchen von Geräten, deren Identity Certificate widerrufen wurde, werden Alerts erzeugt. [Ser23b]

AWS IoT Analytics

AWS IoT Analytics ermöglicht die Durchführung von Datenanalysen auf großen Mengen insbesondere unstrukturierter Daten. Daten der Geräte werden gefiltert, transformiert und angereichert und anschließend als Zeitreihe gespeichert. Analysen auf den Daten sind sodann einmalig oder wiederholt nach Zeitplan möglich, wobei SQL-Abfragen oder ML-Techniken angewendet werden können. [Ser23b]

AWS IoT SiteWise

AWS IoT SiteWise stellt im industriellen Umfeld ein Gateway dar, das die von Sensoren und Aktoren über MQTT-Nachrichten bzw. APIs übertragenen Daten aggregiert, speichert, organisiert und überwacht. Der Datentransfer zwischen on-premise-Datenspeichern und AWS kann so automatisiert werden. [Ser23b]

AWS IoT Twin Maker

AWS IoT Twin Maker kann zur Erstellung von in den vorangegangenen Kapitel dargestellten „digitalen Zwillingen“ physischer bzw. digitaler Systeme verwendet werden. Hierzu werden Daten von Sensoren, Kameras und geschäftlichen Anwendungen herangezogen. Für den Nutzen digitaler Zwillinge sei auf das entsprechende Kapitel verwiesen. [Ser23b]

1.3.4 Evaluation der vorgestellten Angebote

Auf Basis der in den vorherigen Abschnitten dargestellten Angebote und der in der Literatur identifizierten Kriterien soll zur Abrundung der Untersuchung eine quantitative Analyse beider Angebote vorgenommen werden. Hierzu werden - aufgrund ihrer guten Operationalisierbarkeit - die Indikatoren Pricing, Service-Level-Vereinbarungen, Skalierbarkeit, Verwaltung heterogener Daten sowie Node Identity verwendet und jeweils auf die Angebote von Microsoft und Amazon angewendet.

	Microsoft Azure IoT	Amazon AWS IoT
Pricing	teurer [Kau+21]	preiswerter [Kau+21]
SLA	ja (99,9% [Mic24d])	ja (99,9% [Ser22])
Skalierbarkeit	horizontal [Mic23b] & vertikal [Mic23f]	ja [Ser24b]
Heterogene Daten	ja, via Stream Analytics [Mic23i]	ja [Ser24c]
Zahlreiche Endpunkte	ja [Mic23h]	ja [Ser24a]
Gesamt	4	5

Tabelle 1.1: Gegenüberstellung der unterstützten Features von Azure IoT und AWS IoT

Wie die Untersuchung zeigt, ist Amazon AWS auf Basis der gewählten Kriterien als das „bessere“ - da preiswertere - Angebot anzusehen. Dies kann jedoch nicht als generelle Handlungsempfehlung gesehen werden, sondern hängt stets vom konkreten Anwendungsfall der zu realisierenden IoT-Lösung ab. Beispielsweise bietet Microsoft Azure mit IoT Central einen Solution Accelerator an, welcher wesentliche Anforderungen an eine IoT-Anwendung bereits erfüllt und somit die Entwicklungskosten signifikant senken könnte, sofern die Verwendung für den konkreten Anwendungsfall in Frage kommt. Diese Untersuchung kann allenfalls einen Beitrag zu einer entsprechenden Beschreibung leisten.

1.4 Herausforderungen der Nutzung von Cloud Computing im IoT-Umfeld

Die Nutzung von Cloud Computing im IoT-Umfeld ist notwendige Voraussetzung zur Bereitstellung der vorgestellten Funktionsumfänge. Es wurde anhand der vorliegenden Untersuchung eine Evaluierung der Angebote „Azure IoT Hub“ sowie AWS IoT Central durchgeführt, welche die besonderen Anforderungen von IoT-Lösungen abdecken können. Zur Ergänzung der vorliegenden Untersuchung soll hier, neben den eingangs bereits dargestellten *Potenzialen* wie die Verbesserung der Wertschöpfung durch Big Data Analytics, auf Herausforderungen eingegangen werden, die die Nutzung entsprechender Dienste mit sich bringt.

1.4.1 Sicherheit

Der rasante Anstieg der Zahl miteinander verbundener Geräte bedingt auch den Schutz dieser Infrastrukturen vor Schwachstellen und Bedrohungen. IoT-Malware ist bereits am Markt verbreitet und nutzt (u. a.) schwache Login-Daten und veraltete Softwarestände als Angriffsvektor aus. Aufgrund der niedrigen Rechenleistung einzelner IoT-Geräte ist das Ziel die Infektion einer großen Zahl von Geräten zur Bildung von Botnetzen. 2022 wurden rund 112 Millionen Malware-Attacken auf IoT-Geräte verzeichnet [Sta23]. Das BSI gibt hierzu an, dass Cybersicherheit bei der Entwicklung von IoT-Lösungen ein nachrangig beachtetes Ziel ist. Kurze Produktzyklen, Kosten und effektive Herstellungsprozesse führen zu einer Vernachlässigung [Sic17].

In der Standardsetzung wird diesem (Negativ-)Trend mit der Etablierung entsprechender Normen begegnet. So sieht etwa die ETSI-Norm EN 303 645 „baseline requirements“ für Consumer-IoT-Lösungen vor [ETS20]. Hierzu zählen u. a. das Verbot von Standardpasswörtern, geeignete Verschlüsselung dieser und ein Schutz vor Brute-Force-Attacken. Software-Updates müssen, wo sinnvoll, möglich und leicht durchzuführen sein. Netzwerkkommunikation muss verschlüsselt erfolgen und generell nur so wenige Angriffsvektoren wie möglich zulassen („least privilege“). Gegen Ausfälle sollten Geräte besonders gehärtet sein (Weiterbetrieb der lokalen Funktion auch bei Netzwerkausfall). Schließlich muss es dem Anwender leicht möglich sein, seine Benutzerdaten zu löschen. Überdies sind Hersteller auch etwa über Art. 32 der DSGVO zur Einhaltung „technisch-organisatorischer Maßnahmen“ verpflichtet, die den Schutz personenbezogener Daten gewährleisten. Das BSI empfiehlt neben den o. g. Softwareupdates und physischem Zugriffsschutz auf das Produkt auch eine sichere Konfiguration des Heimnetzwerks (Nutzung einer Firewall, Einrichtung eines VPNs bzw. getrennten Netzsegments, Blockierung ausgehender Verbindungen) bzw. generell einen bewussten Einsatz von IoT-Lösungen, insbesondere solcher, die Daten entfernt speichern [Sic23b].

Für IoT-Anwendungen in kritischen Infrastrukturen (Grundversorgung, Verkehrsinfrastruktur, Klimaschutz) wurde das Projekt „RIOT“ (resiliente IoT) durch das BSI gegründet. Durch die Nutzung

redundanter Kommunikationstechnologien oder der Nutzung von Techniken wie der Blockchain oder KI soll die Sicherheit, Verfügbarkeit, Robustheit und Zuverlässigkeit von IoT-Anwendungen verbessert und entsprechende hochverfügbare, sichere Komponenten für und mit Kommunen, Herstellern, Mobilfunkanbietern oder Fachverbänden entwickelt werden. [Sic23a]

1.4.2 Vendor Support

Das Problem des Herstellersupports kann auf zweierlei Arten betrachtet werden. Einerseits erwartet der Nutzer einer IoT-Lösung, dass ihm der gewohnte (hybride) Funktionsumfang langfristig bereitsteht. Gleichzeitig muss auch ein Hersteller, welcher Leistungen bei einem Cloud-Provider einkauft, sich versichern, dass die erforderlichen Leistungen in hinreichender Qualität und Performance bereitstehen. Wie das in der Untersuchung benannte Beispiel der Google Cloud Platform zeigt, stellt die Abschaltung von Diensten in der Praxis durchaus ein relevantes Risiko dar. Zwar lag im Falle von Google IoT Core etwa ein Jahr zwischen der Ankündigung und der tatsächlichen Abschaltung [Men22], gleichzeitig hat die sicherheitstechnische Betrachtung im vorangegangenen Abschnitt gezeigt, dass Hersteller von IoT-Lösungen ggf. keine entsprechenden Software-Updates zur Anpassung der Cloud-Endpunkte ausliefern, zumal eine IoT-Lösung, wie ebenfalls bereits gezeigt, i. d. R. immer in Verbindung mit der konkreten Cloud-Lösung entwickelt wird, was den Schwenk auf eine andere Plattform ggf. erheblich beeinträchtigt oder komplett verhindert.

Dem Herstellersupport im Verhältnis Endkunde - Hersteller der IoT-Lösung soll hier aus betriebswirtschaftlicher Perspektive Raum gegeben werden. Wie Fleisch et al. zeigen, ist das Angebot einer IoT-Lösung nur im Sinne eines nachhaltigen Geschäftsmodells sinnvoll. In Abhängigkeit davon, - ob nur das Produkt monetarisiert wird und die dahinterliegenden Cloud-Dienste jedoch für den Nutzer kostenfrei sind (product play), - ob das Produkt stark vergünstigt bzw. umsonst angeboten wird und ein Abonnement für den Cloud-Dienst abgeschlossen werden muss (service play), - oder ob es sich aus einer Kombination dieser Ansätze handelt (hybrid play), kann ein Hersteller verschiedene Strategien wählen, das Geschäftsmodell nachhaltig zu gestalten. Im Falle des product plays bestehen mögliche Handlungsoptionen entweder in der Minimierung der Dienstkosten (was vertraglich verbindlich mit dem Cloud-Anbieter zu regeln wäre), oder in der künstlichen Begrenzung der Produktlebensdauer, bevor der (Weiter-)Betrieb der IoT-Lösung für den Hersteller unwirtschaftlich wird. Im Gegensatz zur o. g. Perspektive, bei der der Cloud-Anbieter seine Leistung einstellt, wird hier jedoch durch den Hersteller der Zugang zur Cloud-Plattform unterbunden.

1.4.3 Geopolitische Spannungen

Eine abschließende Herausforderung entstammt der von Statista durchgeführten Marktanalyse. Hier wird insbesondere der russische Angriffskrieg auf die Ukraine als Herausforderung für das IoT-Umfeld beschrieben. Problematisch stellt sich die (allgemeine) Halbleiterknappheit dar, die durch die Kriegshandlungen noch verschärft wurden, da beide Länder wichtige Rohstofflieferanten für Halbleiter darstellen. Zudem führen steigende Rohstoffpreise (Öl und Gas) und die hiermit gestiegene Inflationsrate zu einem Nachfragerückgang für IoT-Lösungen insbesondere im Consumer-Umfeld, wo sie, wie beschrieben, nicht zwingend als notwendig angesehen werden. Unternehmen wiederum schichten aufgrund gestiegener Preise ggf. Investitionen um. Schließlich kann die Bildung neuer bzw. veränderter Bündnisse dazu führen, dass für übergreifende Technologie-Standards keine Einigung erzielt werden kann. Dies behindert die Bildung eines globalen IoT-Ökosystems und beeinträchtigt somit das globale Wachstum von IoT-Lösungen und die Herbeiführung von Interoperabilität [Sta23]

1.5 Fazit, Diskussion und Ausblick

Die vorliegende Ausarbeitung hat gezeigt, dass das Aufkommen „smarter“, mit dem Internet verbundener Geräte aller Art sowohl für private Verbraucher als auch für industrielle Fertigungs- und Wertschöpfungsprozesse einen bedeutenden Mehrwert darstellt; überdies hat das Themenfeld im Laufe der letzten 20 Jahre auch an akademischer Relevanz gewonnen. Die Architektur einer solchen IoT-Lösung bezieht dabei auch stets Cloud Computing-Dienste mit ein, etwa um die Geräteflotte zu verwalten oder aus den erzeugten Daten Muster und Erkenntnisse zu generieren. Trends wie 5G oder künstliche Intelligenz beeinflussen die Entwicklung, erwähnenswert ist auch insbesondere die Dezentralisierung der Daten(vor)verarbeitung oder die Nutzung von IoT-Lösungen für „digitale Zwillinge“. Um diese Nutzungspotenziale sinnvoll realisieren zu können, sind Hersteller auf leistungsfähige Cloud-Plattformen angewiesen, die die Besonderheiten von IoT-Lösungen angemessen berücksichtigen können. Im Rahmen dieser Ausarbeitung wurden die Angebote der Hyperscaler Microsoft und Amazon vertieft unter verschiedenen Gesichtspunkten (Kosten, Skalierbarkeit etc.) untersucht - als führend wurde das Angebot von Amazon identifiziert. Gleichzeitig stellt die Nutzung von IoT Hersteller und Anwender vor Herausforderungen - zu nennen sind Sicherheitsrisiken, die Gewährleistung eines langfristigen Supports oder auch durch aktuelle geopolitische Entwicklungen verursachte Beeinträchtigungen wie Preissteigerungen oder Lieferkettenprobleme.

Anzumerken ist, dass aufgrund des begrenzten Umfangs der Arbeit und dem gleichzeitigen Anspruch der Autoren, einen möglichst umfassenden Überblick über das Themenfeld zu vermitteln, nur zwei IoT-Plattformen vertieft beschrieben bzw. analysiert werden konnten. Hierbei ist auch anzumerken, dass die hierzu verwendeten Quellen in einigen Fällen möglicherweise nicht einem „wissenschaftlichen“ Anspruch genügen, da es sich nicht um begutachtete wissenschaftliche Quellen handelt. Um dem zu begegnen, haben die Autoren die Verwendung möglichst objektiver Quellen angestrebt, zumal einige Fachbücher und Konferenzbeiträge in die Untersuchung einbezogen werden konnten.

Im Sinne eines Ausblicks ist erkennbar, dass die Kombination von IoT-Lösungen und Cloud Computing auch künftig ein relevantes Themenfeld mit betriebs- bzw. volkswirtschaftlichem Wachstumspotential darstellt. Die Entwicklung weiterer Use-Cases, Marktsegmente sowie der generelle Anstieg des weltweiten Datenvolumens rechtfertigen auch in Zukunft Untersuchungen der Thematik. Hierbei können weitere Cloud-Plattformen, insbesondere weniger verbreitete, evaluiert werden oder ein allgemeines Framework zur ganzheitlichen Beurteilung von IoT-Cloudplattformen entwickelt werden. Nicht zuletzt wird sich auch die sicherheitstechnische Betrachtung von IoT-Geräten, vor allem deren Härtung, zu einem relevanten Thema entwickeln.

Literatur

- [AIM10] Luigi Atzori, Antonio Iera und Giacomo Morabito. „The Internet of Things: A survey“. In: *Computer Networks* 54.15 (Okt. 2010), S. 2787–2805. ISSN: 1389-1286. doi: [10.1016/j.comnet.2010.05.010](https://doi.org/10.1016/j.comnet.2010.05.010).
- [Al-+15] Ala Al-Fuqaha u. a. „Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications“. In: *IEEE Communications Surveys & Tutorials* 17.4 (2015), S. 2347–2376. ISSN: 2373-745X. doi: [10.1109/comst.2015.2444095](https://doi.org/10.1109/comst.2015.2444095).
- [Ash09] Kevin Ashton. *That 'Internet of Things' Thing*. RFID Journal. 2009. URL: <https://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf> (besucht am 27.01.2024).
- [Con06] J.P. Conti. „The Internet of things“. In: *Communications Engineer* 4.6 (Dez. 2006), S. 20–25. ISSN: 1741-0452. doi: [10.1049/ce:20060603](https://doi.org/10.1049/ce:20060603).
- [Ert21] Wolfgang Ertel. *Grundkurs Künstliche Intelligenz. Eine praxisorientierte Einführung*. 5. Auflage. Springer eBook Collection. Wiesbaden: Springer Vieweg, 2021. 1422 S. ISBN: 9783658320751.
- [ETS20] ETSI. *ETSI EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements*. 2020. URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.
- [EW16] Michael Ehret und Jochen Wirtz. „Unlocking value from machines: business models and the industrial internet of things“. In: *Journal of Marketing Management* 33.1-2 (Nov. 2016), S. 111–130. doi: [10.1080/0267257x.2016.1248041](https://doi.org/10.1080/0267257x.2016.1248041).
- [Fas16] Daniel; Andreas Meier Fasel. *Big Data. Grundlagen, Systeme und Nutzungspotenziale*. Hrsg. von Andreas Meier. Edition HMD Ser. Description based on publisher supplied metadata and other sources. Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2016. 1384 S. ISBN: 9783658115890.
- [Fin18] Bundesanstalt für Finanzdienstleistungsaufsicht. *Big Data trifft auf künstliche Intelligenz - Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen*. 2018. URL: https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdatstudie.pdf.
- [Ful+20] Aidan Fuller u. a. „Digital Twin: Enabling Technologies, Challenges and Open Research“. In: *IEEE Access* 8 (2020), S. 108952–108971. ISSN: 2169-3536. doi: [10.1109/access.2020.2998358](https://doi.org/10.1109/access.2020.2998358).
- [FWW14] Edgar Fleisch, Markus Weinberger und Felix Wortmann. *Business Models and the Internet of Things*. Bosch Internet of Things & Services Lab. 2014. URL: https://www.iot-lab.ch/wp-content/uploads/2014/11/EN_Bosch-Lab-White-Paper-GM-im-IOT-1_3.pdf (besucht am 20.10.2023).
- [GKC04] Neil Gershenfeld, Raffi Krikorian und Danny Cohen. „The Internet of Things“. In: *Scientific American* 291.4 (Okt. 2004), S. 76–81. ISSN: 0036-8733. doi: [10.1038/scientificamerican1004-76](https://doi.org/10.1038/scientificamerican1004-76).
- [Gla15] Kyle Ebersold;Richard Glass. „THE IMPACT OF DISRUPTIVE TECHNOLOGY: THE INTERNET OF THINGS“. In: *Issues In Information Systems* (2015). ISSN: 1529-7314. doi: [10.48009/4_iis_2015_194-201](https://doi.org/10.48009/4_iis_2015_194-201). URL: https://doi.org/10.48009/4_iis_2015_194-201.

- [Goo22] Alfonso Velosa;Eric Goodness. *Magic Quadrant for Global Industrial IoT Platforms*. 2022. URL: <https://www.gartner.com/doc/reprints?id=1-2BY92VID&ct=221209&st=sb>.
- [Goo23] Google. *Cloud IoT Core*. de. 2023. URL: <https://cloud.google.com/iot-core?hl=de> (besucht am 13. 02. 2024).
- [Gra12] Peter Mell; Timothy Grance. *The NIST Definition of Cloud Computing*. 2012. URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>.
- [GS18] Kevin Grünberg und Wolfram Schenck. „A Case Study on Benchmarking IoT Cloud Services“. In: *Cloud Computing – CLOUD 2018*. Springer International Publishing, 2018, S. 398–406. ISBN: 9783319942957. doi: [10.1007/978-3-319-94295-7_28](https://doi.org/10.1007/978-3-319-94295-7_28).
- [Kam20] Stylianos Kampakis. *The decision maker's handbook to data science. A guide for non-technical executives, managers, and founders*. Second edition. Springer eBook Collection. [Berkeley, CA]: Apress, 2020. 115621 S. ISBN: 9781484254943.
- [Kau+21] Prakarsh Kaushik u. a. „Cloud Computing and Comparison based on Service and Performance between Amazon AWS, Microsoft Azure, and Google Cloud“. In: *2021 International Conference on Technological Advancements and Innovations (ICTAI)*. IEEE, Nov. 2021. doi: [10.1109/ictai53825.2021.9673425](https://doi.org/10.1109/ictai53825.2021.9673425).
- [Kom22] Europäische Kommission. *BERICHT DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT -Endgültiger Bericht - Sektoruntersuchung zum Internet der Dinge für Verbraucher*. 2022. URL: https://competition-policy.ec.europa.eu/system/files/2022-01/internet-of-things_final_report_2022_de.pdf.
- [Lew23] Marco Lewandowski. *IoT vs. IIoT - Unterschiede von Konsumentenprodukten und industriellen Systemen*. en-GB. Apr. 2023. URL: <https://www.swms-consulting.de/en/iot-vs-iiot-unterschiede-von-konsumentenprodukten-und-industriellen-systemen/> (besucht am 11.02.2024).
- [Men22] Rainald Menge-Sonnentag. *Internet der Dinge: Google schickt seine IoT-Cloud aufs Abstellgleis*. de. Aug. 2022. URL: <https://www.heise.de/news/Internet-der-Dinge-Google-schickt-seine-IoT-Cloud-aufs-Abstellgleis-7222369.html> (besucht am 13.02.2024).
- [Mic18] Microsoft. *IoT device authentication options | Azure Blog | Microsoft Azure*. de-DE. Okt. 2018. URL: <https://azure.microsoft.com/de-de/blog/iot-device-authentication-options/> (besucht am 07.02.2024).
- [Mic20] Microsoft. *24Storage: Removing physical interactions to empower customer service*. en. 2020. URL: <https://customers.microsoft.com/en-us/story/852285-24storage-azure-en-sweden> (besucht am 07.02.2024).
- [Mic21] Microsoft. *Clean Energy Fuels runs greener, boosts efficiency with Dynamics 365*. en. 2021. URL: <https://customers.microsoft.com/en-us/story/859804-clean-energy-fuels-energy-dynamics-365> (besucht am 07.02.2024).
- [Mic22a] Microsoft. *Azure Stream Analytics autoscale streaming units - Azure Stream Analytics*. en-us. Dez. 2022. URL: <https://learn.microsoft.com/en-us/azure/stream-analytics/stream-analytics-autoscale> (besucht am 09.02.2024).

- [Mic22b] Microsoft. *Grupo Bimbo takes a bite out of production costs with Azure IoT throughout factories.* en. 2022. URL: <https://customers.microsoft.com/en-us/story/1442585718978307558-grupo-bimbo-consumer-goods-azure-iot> (besucht am 07.02.2024).
- [Mic22c] Microsoft;Intel. *IoT Signals - Manufacturing Spotlight.* 2022. URL: <https://clouddamcdnprodep.azureedge.net/gdc/gdcmAYP6m/original>.
- [Mic23a] Microsoft. *Architectural concepts in Azure IoT Central - Azure IoT Central.* en-us. Feb. 2023. URL: <https://learn.microsoft.com/en-us/azure/iot-central/core/concepts-architecture> (besucht am 05.02.2024).
- [Mic23b] Microsoft. *Azure IoT Hub scaling.* en-us. März 2023. URL: <https://learn.microsoft.com/en-us/azure/iot-hub/iot-hub-scaling> (besucht am 18.02.2024).
- [Mic23c] Microsoft. *Grundlegendes zu Azure IoT Hub-Gerätezwilligen.* de-de. März 2023. URL: <https://learn.microsoft.com/de-de/azure/iot-hub/iot-hub-devguide-device-twins> (besucht am 09.02.2024).
- [Mic23d] Microsoft. *Grundlegendes zu direkten Azure IoT Hub-Methoden.* de-de. März 2023. URL: <https://learn.microsoft.com/de-de/azure/iot-hub/iot-hub-devguide-direct-methods> (besucht am 09.02.2024).
- [Mic23e] Microsoft. *Grundlegendes zum Azure IoT Hub-C2D-Messaging.* de-de. März 2023. URL: <https://learn.microsoft.com/de-de/azure/iot-hub/iot-hub-devguide-messages-c2d> (besucht am 09.02.2024).
- [Mic23f] Microsoft. *Übersicht über IoT Hub Device Provisioning Service.* de-de. März 2023. URL: <https://learn.microsoft.com/de-de/azure/iot-dps/about-iot-dps> (besucht am 05.02.2024).
- [Mic23g] Microsoft. *Übersicht über IoT Hub Device Provisioning Service.* de-de. März 2023. URL: <https://learn.microsoft.com/de-de/azure/iot-dps/about-iot-dps> (besucht am 09.02.2024).
- [Mic23h] Microsoft. *Understand Azure IoT Hub quotas and throttling.* en-us. Aug. 2023. URL: <https://learn.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-quotas-throttling> (besucht am 18.02.2024).
- [Mic23i] Microsoft. *Understand inputs for Azure Stream Analytics - Azure Stream Analytics.* en-us. März 2023. URL: <https://learn.microsoft.com/en-us/azure/stream-analytics/stream-analytics-add-inputs> (besucht am 18.02.2024).
- [Mic23j] Microsoft. *Verarbeiten von IoT-Datenströmen in Echtzeit mit Azure Stream Analytics - Azure Stream Analytics.* de-de. Aug. 2023. URL: <https://learn.microsoft.com/de-de/azure/stream-analytics/stream-analytics-get-started-with-azure-stream-analytics-to-process-data-from-iot-devices> (besucht am 09.02.2024).
- [Mic23k] Microsoft. *Was ist Azure IoT Central? - Azure IoT Central.* de-de. Juni 2023. URL: <https://learn.microsoft.com/de-de/azure/iot-central/core/overview-iot-central> (besucht am 05.02.2024).
- [Mic24a] Microsoft. *Azure IoT-Produkte und -Dienste | Microsoft Azure.* de-DE. 2024. URL: <https://azure.microsoft.com/de-de/products/category/iot> (besucht am 05.02.2024).
- [Mic24b] Microsoft. *IoT Hub | Microsoft Azure.* de-DE. 2024. URL: <https://azure.microsoft.com/de-de/products/iot-hub> (besucht am 11.02.2024).

- [Mic24c] Microsoft. *Send device telemetry to Azure IoT Hub quickstart*. en-us. Jan. 2024. URL: <https://learn.microsoft.com/en-us/azure/iot-develop/quickstart-send-telemetry-iot-hub> (besucht am 07.02.2024).
- [Mic24d] Microsoft. *Service Level Agreement for Microsoft Online Services*. 2024. URL: [https://view.officeapps.live.com/op/view.aspx?src=https://wwlpdocumentsearch.blob.core.windows.net/prodv2/OnlineSvcsConsolidatedSLA\(WW\)\(English\)\(February2024\)\(CR\).docx&wdOrigin=BROWSELINK](https://view.officeapps.live.com/op/view.aspx?src=https://wwlpdocumentsearch.blob.core.windows.net/prodv2/OnlineSvcsConsolidatedSLA(WW)(English)(February2024)(CR).docx&wdOrigin=BROWSELINK).
- [Mic24e] Microsoft. *So finden Sie den passenden Cloud-Dienstanbieter | Microsoft Azure*. de-DE. 2024. URL: <https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/choosing-a-cloud-service-provider> (besucht am 11.02.2024).
- [Mic24f] Microsoft. *Was ist künstliche Intelligenz? | Microsoft Azure*. de-DE. 2024. URL: <https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-artificial-intelligence> (besucht am 11.02.2024).
- [Mic24g] Microsoft. *Was sind Big-Data-Analysen? | Microsoft Azure*. de-DE. 2024. URL: <https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-big-data-analytics> (besucht am 11.02.2024).
- [Mis22] Sanjay Misra. *Artificial Intelligence for Cloud and Edge Computing*. Hrsg. von Amit Kumar Tyagi, Vincenzo Piuri und Lalit Garg. Internet of Things Ser. Description based on publisher supplied metadata and other sources. Cham: Springer International Publishing AG, 2022. 1358 S. ISBN: 9783030808211.
- [MU20] Aina'u Shehu Muhammed und Derya Ucuz. „Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives“. In: *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, Juni 2020. DOI: [10.1109/isdfs49300.2020.9116254](https://doi.org/10.1109/isdfs49300.2020.9116254).
- [NM18] Klaus North und Ronald Maier. „Wissen 4.0 – Wissensmanagement im digitalen Wandel“. In: *HMD Praxis der Wirtschaftsinformatik* 55.4 (Mai 2018), S. 665–681. ISSN: 2198-2775. DOI: [10.1365/s40702-018-0426-6](https://doi.org/10.1365/s40702-018-0426-6).
- [Ray16] Partha Pratim Ray. „A survey of IoT cloud platforms“. In: *Future Computing and Informatics Journal* 1.1–2 (Dez. 2016), S. 35–46. ISSN: 2314-7288. DOI: [10.1016/j.fcij.2017.02.001](https://doi.org/10.1016/j.fcij.2017.02.001).
- [Sat17] Mahadev Satyanarayanan. „The Emergence of Edge Computing“. In: *Computer* 50.1 (Jan. 2017), S. 30–39. ISSN: 0018-9162. DOI: [10.1109/mc.2017.9](https://doi.org/10.1109/mc.2017.9).
- [SD16] Weisong Shi und Schahram Dustdar. „The Promise of Edge Computing“. In: *Computer* 49.5 (Mai 2016), S. 78–81. ISSN: 0018-9162. DOI: [10.1109/mc.2016.145](https://doi.org/10.1109/mc.2016.145).
- [Ser22] Amazon Web Services. *AWS IoT Core Service Level Agreement*. 2022. URL: <https://aws.amazon.com/de/iot-core/sla/>.
- [Ser23a] Amazon Web Services. *AWS IoT Greengrass Documentation*. 2023. URL: <https://docs.aws.amazon.com/greengrass/>.
- [Ser23b] Amazon Web Services. *How AWS IoT works*. 2023. URL: <https://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html>.
- [Ser23c] Amazon Web Services. *IoT-Plattformen – Amazon & das "Allesnetz" – Amazon Web Services (AWS)*. de-DE. 2023. URL: <https://aws.amazon.com/de/iot/> (besucht am 13.02.2024).

- [Ser23d] Amazon Web Services. *What is AWS IoT?* 2023. URL: <https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>.
- [Ser24a] Amazon Web Services. *AWS IoT*. 2024. URL: <https://aws.amazon.com/de/iot/>.
- [Ser24b] Amazon Web Services. *AWS IoT Core*. 2024. URL: <https://aws.amazon.com/de/iot-core/>.
- [Ser24c] Amazon Web Services. *Was ist der Unterschied zwischen strukturierten Daten und unstrukturierten Daten?* 2024. URL: <https://aws.amazon.com/de/compare/the-difference-between-structured-data-and-unstructured-data/>.
- [Shi+16] Weisong Shi u. a. „Edge Computing: Vision and Challenges“. In: *IEEE Internet of Things Journal* 3.5 (Okt. 2016), S. 637–646. ISSN: 2327-4662. DOI: [10.1109/jiot.2016.2579198](https://doi.org/10.1109/jiot.2016.2579198).
- [Sic17] Bundesamt für Sicherheit in der Informationstechnik. *Sicherheit von Geräten im Internet der Dinge*. 2017. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_128.pdf?__blob=publicationFile&v=3.
- [Sic23a] Bundesamt für Sicherheit in der Informationstechnik. *Projekt RIOT*. de. 2023. URL: <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G/KoPa45/Sicherheit-und-Resilienz-5G-6G/TSP4-RIOT/TSP4-RIOT.html?nn=1090878> (besucht am 11.02.2024).
- [Sic23b] Bundesamt für Sicherheit in der Informationstechnik. *Smarthome – den Wohnraum sicher vernetzen*. de. 2023. URL: <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/smart-home.html?nn=131484> (besucht am 11.02.2024).
- [Sis+18] Emiliano Sisinni u. a. „Industrial Internet of Things: Challenges, Opportunities, and Directions“. In: *IEEE Transactions on Industrial Informatics* 14.11 (Nov. 2018), S. 4724–4734. ISSN: 1941-0050. DOI: [10.1109/tii.2018.2852491](https://doi.org/10.1109/tii.2018.2852491).
- [Sta19] Robert Stackowiak. *Azure Internet of Things Revealed. Architecture and Fundamentals*. Description based on publisher supplied metadata and other sources. Berkeley, CA: Apress L. P., 2019. 1214 S. ISBN: 9781484254707.
- [Sta22] Statista. *Global IoT and non-IoT connections 2010-2025*. en. 2022. URL: <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/> (besucht am 13.02.2024).
- [Sta23] Statista. *Internet der Dinge: Marktdaten & -analyse*. de. 2023. URL: <https://de.statista.com/statistik/studie/id/109209/dokument/internet-der-dinge-market-outlook-report/> (besucht am 11.02.2024).
- [Tao+19] Fei Tao u. a. „Digital Twin in Industry: State-of-the-Art“. In: *IEEE Transactions on Industrial Informatics* 15.4 (Apr. 2019), S. 2405–2415. ISSN: 1941-0050. DOI: [10.1109/tii.2018.2873186](https://doi.org/10.1109/tii.2018.2873186).
- [Tas21] Pelin Yildirim Taser. *Emerging trends in IOT and integration with data science cloud computing, and big data analytics*. Hrsg. von Pelin Yildirim Taser. IGI Global, 2021. 122334 S. ISBN: 9781799841876.
- [WF15] Felix Wortmann und Kristina Flüchter. „Internet of Things“. In: *Business Information Systems Engineering* 57.3 (März 2015), S. 221–224. DOI: [10.1007/s12599-015-0383-3](https://doi.org/10.1007/s12599-015-0383-3).

- [Wir18] KPMG AG Wirtschaftsprüfungsgesellschaft. *Rethinking the value chain - A study on AI, humanoids and robots*. 2018. URL: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/09/rethinking-the-value-chain.pdf>.
- [XHL14] Li Da Xu, Wu He und Shancang Li. „Internet of Things in Industries: A Survey“. In: *IEEE Transactions on Industrial Informatics* 10.4 (Nov. 2014), S. 2233–2243. ISSN: 1941-0050. DOI: [10.1109/tnii.2014.2300753](https://doi.org/10.1109/tnii.2014.2300753).