# DLBCSEEIST01\_E

# Übergeordnete Lernziele

Heutzutage werden in der Welt des Internets der Dinge (IoT, Internet of Things) zahlreiche vernetzte Geräte eingesetzt, um die Lebensqualität des Einzelnen zu verbessern. Von Sensoren erfasste Daten werden analysiert, um Erkenntnisse für Unternehmen und Branchen zu gewinnen. Böswillige Akteure und Hacker versuchen, die Schwachstellen von IoT-Geräten und -Systemen auszunutzen, um Zugang zu wertvollen Daten zu erhalten.

Dieses Studienskript beginnt mit der Vermittlung der Grundlagen zum Thema **IoT-Sicherheit**, indem es IoT-Architektur, Schwachstellen, Sicherheitsangriffe und Gegenmaßnahmen auf jeder Ebene von IoT-Systemen beleuchtet. Als Nächstes werden Sie mit dem Konzept „Security by Design“ vertraut gemacht, bei dem Sicherheitsaspekte bereits in den frühen Entwicklungsphasen berücksichtigt werden. Darüber hinaus behandelt dieses Studienskript statische und dynamische Testmethoden, die Code-Schwachstellen von Anwendungen entdecken und verhindern, dass Hacker diese ausnutzen.

Auch die Absicherung von End-to-End-IoT-Lösungen auf den verschiedenen Ebenen Gerät, Netzwerk und Cloud wird untersucht. Die Sicherheitsrisiken und Konstruktionsziele von IoT-Geräten sowie Authentifizierung und Autorisierung als zwei wichtige Konzepte der Betriebssicherheit werden erläutert. Außerdem erhalten Sie Informationen über Bedrohungen für IoT-Dienste und über die Sicherung von Cloud-Lösungen.

Abschließend werden die Konzepte von Big Data, künstlicher Intelligenz und maschinellem Lernen, einschließlich überwachter und unüberwachter Algorithmen, erörtert. Sie werden mehr über die Rolle dieser Algorithmen beim Schutz von IoT-Systemen vor Cyberkriminellen erfahren.

# Lektion 1 – Grundlagen des Internets der Dinge (IoT)

**Lernziele**

Nach dem Abschluss dieser Lektion werden Sie...

... die Hauptbestandteile der IoT-Wertschöpfungskette beschreiben können.

... die Herausforderungen bei der Einrichtung und beim Einsatz von IoT-Lösungen auflisten können.

... in der Lage sein, die Architektur des IoT und die Rolle der einzelnen Schichten im grundlegenden IoT-Technologie-Stack zu erklären.

... den Unterschied zwischen IoT für Konsumenten und industriellem IoT erklären können.

... die wichtigsten Merkmale von industriellen IoT-Anwendungen kennen.

# Grundlagen des Internets der Dinge (IoT)

## Einleitung

Die Fortschritte in der Elektronik und bei Computersystemen im späten zwanzigsten Jahrhundert ermöglichten die Maschine-zu-Maschine-Kommunikation (M2M), bei der Daten und Befehle direkt (Punkt-zu-Punkt) zwischen Geräten und Maschinen übertragen werden können. Die Skalierbarkeit und das Zusammenwirken solcher hardwarebasierten M2M-Netze waren jedoch begrenzt, da alle Geräte die gleichen Kommunikationsprotokolle verwenden mussten. In der hochgradig skalierbaren Welt des Internets der Dinge (IoT) kann jedoch so gut wie jedes „Ding“ – von einem einfachen Lichtsensor oder einem intelligenten Toaster bis hin zu sehr fortschrittlichen Robotern in intelligenten Fabriken – mit dem Internet verbunden werden und auf diesem Weg mit anderen intelligenten Geräten und Nutzer:innen in der Welt kommunizieren.

## Einleitung in das IoT

 Spezielle Kommunikationstechnologien wie **Low-Power-Wide-Area-Networks** (LPWAN) ermöglichen viele IoT-Einsatzfälle, indem sie die intelligenten Geräte in die Lage versetzen, monatelang mit kleinen Batterien zu arbeiten, so dass sie Daten mit der Cloud und anderen IoT-Geräten austauschen können, ohne dass eine regelmäßige Wartung oder ein Batteriewechsel erforderlich ist. Diese kostengünstigen IoT-Geräte mit begrenzten Ressourcen im LPWAN sind jedoch anfällig für Sicherheitsbedrohungen, da Cyberangreifer:innen sich in der Regel auf die schwächste Komponente der Infrastruktur konzentrieren.

**Low-power Wide-area (LPWA)**

Eine Gruppe zellularer und nicht zellularer Kommunikationstechnologien mit geringer Leistung und großer Reichweite, die in vielen IoT-Anwendungen eingesetzt werden.

Darüber hinaus sind leistungsstarke Datenanalysetools in der Lage, die riesigen Datenmengen zu analysieren, die von den zahlreichen IoT-Geräten in Smart Homes, intelligenten Fabriken, intelligenten Stromnetzen, Wearables usw. empfangen werden, und daraus Erkenntnisse für Einzelpersonen, Unternehmen und Organisationen zu gewinnen.

IoT-Einsatzfälle verbinden viele Dinge miteinander und bringen viele Vorteile für Einzelpersonen, Unternehmen und Gesellschaften durch ein System mit vier Hauptelementen, die zusammenarbeiten, um die Ziele einer vernetzten Welt zu erreichen: Dinge, Menschen (Entwickler:innen, Netzbetreiber und Nutzer:innen), Daten (Informationen, die von Sensoren erfasst und an die Cloud übertragen werden, sowie Befehle an das intelligente Objekt) und Prozesse (Farshad Firouzi, 2020). Im Konzept des IoT muss ein Gerät oder Ding die folgenden vier Merkmale aufweisen, um als IoT-Gerät oder intelligentes Objekt zu gelten (David Hanes, 2017):

1. Sensor(en) und Aktor(en) zur Interaktion mit der physischen Welt.
2. Eine Kommunikationseinheit zur Verbindung des intelligenten Objekts mit dem Internet.
3. Eine Stromquelle zur Versorgung der Sensoren, Kommunikations- und Verarbeitungssysteme.
4. Eine Prozessoreinheit zur Verarbeitung und Analyse der von den Sensoren gesammelten Daten und zur Steuerung anderer Systeme wie Energie- und Kommunikationseinheiten.

### Auswirkungen des IoT

In naher Zukunft wird sich das IoT auf jeden Aspekt unseres Lebens auswirken, sei es auf die Art und Weise, wie wir unsere Gesundheit überwachen, wie wir zur Arbeit kommen oder wie wir unsere Einkäufe erledigen. Auch für Organisationen und Unternehmen bringt es viele Vorteile mit sich. Die sich aus der Analyse der IoT-Daten ergebenden Maßnahmen und Ergebnisse können die Produktivität durch eine effektivere Verwaltung der Ressourcen steigern. Das IoT schafft Transparenz, indem es den Standort von Vermögenswerten und den Status von Prozessen, wie z. B. Produktionslinien, identifiziert. Die IoT-Rule-Engines in Verbindung mit künstlicher Intelligenz (KI) automatisieren und erhöhen die Genauigkeit von Prozessen und sagen Ausfälle in Systemen voraus, um Probleme zu vermeiden. Darüber hinaus kann das IoT bei der Bewältigung von Sicherheitsproblemen helfen, indem es gefährliche Situationen und Umgebungsfaktoren zuverlässiger und schneller erkennt (Farshad Firouzi, 2020).

### IoT-Wertschöpfungskette

Jede IoT-Lösung besteht aus verschiedenen Komponenten und Bausteinen, die von einer Reihe von Unternehmen entwickelt werden. Diese Komponenten werden als IoT-Wertschöpfungskette bezeichnet und spielen verschiedene Rollen, die den Endnutzer:innen der Lösung einen gewissen Mehrwert bieten. Zu den Komponenten einer IoT-Wertschöpfungskette gehören Hardware, Konnektivität, Plattform und Anwendung (Rebbeck, 2020).

Die IoT-Wertschöpfungskette



Quelle: Reza Vahidnia (2022)

Die Hardware umfasst eine Reihe von Sensoren/Aktoren, die Daten erfassen/verarbeiten, sowie die für die Kommunikation verwendete Hardware (d. h. Chipsätze und SIM-Karten für die Verbindung des Geräts mit dem Netzwerk). Die Konnektivitätskomponente (z. B. ein Mobilfunknetzbetreiber) ist für die Übertragung der Daten und Befehle zwischen den Sensoren/Aktoren und dem Backend (d. h. den Servern, welche die Daten sammeln) zuständig. Die IoT-Plattform (z. B. ThingsBoard, Microsoft Azure oder Amazon Web Services) gilt als zentrales Rückgrat des IoT und dient dazu, die Lücke zwischen Hardware und Anwendungen zu schließen, indem sie Entwickler:innen eine Kombination gebrauchsfertiger Funktionen zur Verfügung stellt. Das Anwendungselement ist der Bereich, in dem die Entwickler:innen ihren Anteil am IoT erhöhen, indem sie nützliche Schnittstellen für die Nutzer:innen schaffen.

### IoT-Cluster

Das IoT kann in verschiedene Cluster eingeteilt werden, und zwar in Verticals, Einsatzfälle und Anwendungen. Diese Cluster werden in der Abbildung unten dargestellt.

IoT-Cluster

Quelle: Reza Vahidnia (2022)

Verschiedene IoT-Einsatzfälle haben unterschiedliche Vorteile für verschiedene Branchen und Segmente. Die zu einem bestimmten Branchensegment gehörenden IoT-Einsatzfälle werden einem IoT-Vertical mit eigenen Regulierungsstellen, Verfahren, Protokollen und Normierungsorganisationen zugeordnet (Dian & Vahidnia, 2021). Diese IoT-Einsatzfälle erfordern in der Regel ähnliche Datenspeicher-, Datenverarbeitungs- und Analysefähigkeiten. Die IoT-Einsatzfälle „intelligenter Kühlschrank“ und „intelligente Waschmaschine“ gehören beispielsweise beide zum Vertical „Smart Home“ und dienen dem Komfort der Hausbewohner:innen und der Energieeinsparung. Ein weiteres Beispiel ist die „intelligente Fabrik“, die als IoT-Einsatzfall zur Verringerung menschlicher Fehler und der Betriebskosten in der Industrie angesehen wird.

Jeder IoT-Einsatzfall kann mehrere IoT-Anwendungen umfassen, die ähnliche Lösungen und Software verwenden. Beispielsweise können in dem Einsatzfall „vernetztes Fahrzeug“ Anwendungen für Infotainment, Telematik und Flottenmanagement genutzt werden.

### Herausforderungen für das IoT

Neben den zahlreichen Vorteilen bringen die Einführung und der Einsatz von IoT-Lösungen auch ihre eigenen Herausforderungen mit sich. Dazu gehören:

* **Skalierbarkeit:** Eine enorme Anzahl von IoT-Geräten (bis zu mehreren Millionen Sensoren) muss an das Netz angeschlossen werden. Aus diesem Grund ist IPv4 für den Aufbau von IoT-Netzen möglicherweise nicht ausreichend.
* **Interoperabilität:** IoT-Geräte gibt es von verschiedenen Anbietern, mit unterschiedlichen Normen und Kommunikationsprotokollen. Die Entwicklung eines Netzwerks, das all diese verschiedenen Normen und Protokolle unterstützt, könnte daher eine Herausforderung darstellen.
* **Sicherheit:** Vertrauliche Daten, die von IoT-Sensoren erfasst werden, müssen sicher geschützt werden, während sie vom Sensor erzeugt, von Edge-Geräten verarbeitet, an die Cloud übertragen, in der Datenbank gespeichert, von Menschen, Anwendungen und anderen Diensten abgerufen und von Analysesoftware analysiert werden.
* **Datenschutz:** Privatpersonen und Unternehmen wollen wissen, ob und an wen die gesammelten Daten weitergegeben werden. Aus diesem Grund zögern manche Menschen, IoT-Geräte in ihrem täglichen Leben oder in ihrem Unternehmen einzusetzen.
* **Big Data und Analytik:** Die diversen Arten von Daten, die von verschiedenen Sensoren erfasst werden, müssen richtig aufbereitet und strukturiert werden, bevor sie gespeichert, analysiert und dargestellt werden können.
* **Rechtliches:** Das geistige Eigentum und die Haftung jedes Akteurs im System sollten klar definiert sein.
* **Begrenzte Ressourcen:** Die meisten IoT-Geräte sind einfach und kostengünstig und verfügen nur über begrenzte Speicher-, Leistungs- und Verarbeitungskapazitäten. Daher kann die Implementierung starker Sicherheitsmechanismen auf IoT-Geräten schwierig oder unmöglich sein.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie die vier Hauptkomponenten der IoT-Wertschöpfungskette.

*Hardware*

*Konnektivität*

*Plattform*

*Anwendungen*