

Grundlagen zum Einstieg ins Internet der Dinge

Dipl.-Ing. Günter Obiltschnig
Applied Informatics Software Engineering GmbH

@obiltschnig
guenter.obiltschnig@appinf.com
<http://www.appinf.com>
<http://macchina.io>

1. Begriffserklärung

Das Internet der Dinge (englisch: Internet of Things, kurz IoT) und die damit verbundenen Begriffe Cyber-Physical Systems, Industrie 4.0 und Industrial Internet sind derzeit in aller Munde. Doch was steckt dahinter? Frei nach Wikipedia ist das Internet der Dinge “das Netzwerk physikalischer Objekte (Geräte, Fahrzeuge, Gebäude und andere ‘Dinge’) mit eingebetteter Elektronik, Software, Sensoren und Konnektivität, welches Wertschöpfung und neue Dienste ermöglicht, in dem Daten mit dem Hersteller, Betreiber, oder anderen verbundenen Geräten ausgetauscht werden. Jedes ‘Ding’ ist durch das eingebaute Computersystem eindeutig identifizierbar und kann mit der bestehenden Internet Infrastruktur zusammenarbeiten.”

Von RFID zu IoT

Der Begriff “Internet der Dinge” wurde erstmals 1999 vom Briten Kevin Ashton im Zusammenhang mit RFID Technologie (Funktechnologie zur berührungslosen Identifikation von Objekten) dokumentiert. Die Idee war, physikalische Objekte mit einem RFID Transponder zu versehen, um sie so eindeutig elektronisch identifizierbar zu machen. Jedes physikalische Objekt sollte praktisch ein Gegenstück im „Cyberspace“ haben wobei die Verbindung zwischen realer und virtueller Instanz über eine eindeutigen Identifizierung, etwa in Form einer URL, erfolgt.

Nachdem sich der anfängliche Hype um RFID am Anfang des vorherigen Jahrzehnts recht schnell wieder der Realität – Investitionskosten vs. möglicher Einsparungspotentiale – beugen musste verschwand der Begriff „Internet der Dinge“ für einige Zeit wieder in der Versenkung, bis er Anfang dieses Jahrzehnts in neuer Bedeutung wieder auftauchte.

Über das mobile Internet zum Internet der Dinge

Das Internet der Dinge ist die logische Fortführung einer Entwicklung, die mit der weitläufigen Verbreitung des Internets Mitte der 1990er Jahre begann. Mit der Verfügbarkeit des iPhone und anderer Smart Phones ab 2007, sowie entsprechender Entwicklungen im Mobilfunkbereich machte das Internet den Schritt von örtlich gebundener Verfügbarkeit (PC) hin zu ständiger, mobiler Verfügbarkeit, allerdings immer noch beschränkt auf spezielle Endgeräte (Smart Phones, Tablets). Das Internet der Dinge schlussendlich integriert das

Internet in Dinge, bzw. Geräte und Maschinen des alltäglichen Gebrauchs und macht es somit unabhängig von speziellen Endgeräten.

Exkurs: Von M2M zu IoT

Im Zusammenhang mit dem Internet der Dinge muss auch der Begriff Machine-to-Machine (M2M) erwähnt werden. M2M kann quasi als Vorläufer des Internet der Dinge angesehen werden. Allerdings hatte M2M einen starken Fokus auf proprietäre, GSM/GPRS und später UMTS-basierte Insellösungen und wurde von Mobilfunkanbietern recht schnell als Vehikel entdeckt, um neue Kundensegmente für Mobilfunkverträge, bzw. SIM Karten zu finden. Im Wesentlichen geht es um den Einbau eines Mobilfunk-Modems, bzw. generell eines Netzwerkzugangs, in ein bestehendes Computer-gesteuertes Gerät zum Zwecke der Datenkommunikation, bzw. der Fernwartung, also quasi die Ablösung früher verwendeter Modemverbindungen. In diesem Zusammenhang entwickelten sich auch erste sogenannte „Device Management“ Lösungen und Plattformen, die es einerseits ermöglichen, eine große Anzahl an Netzwerk-tauglichen Geräten zu verwalten, als auch basierend auf den von den Geräten gesendeten Daten, neue Geschäftsanwendungen zu entwickeln. Dabei kommen allerdings weitgehend proprietäre Kommunikationsprotokolle, bzw. Softwareplattformen zum Einsatz.

Der wesentliche Schritt von M2M zum Internet der Dinge ist die Einführung offener Kommunikations- und Interoperabilitätsschnittstellen auf allen Ebenen der Kommunikation, vom Sensor bis zur Cloud, sozusagen „M2M im nächst größeren Kontext“ (Landon Cox, Informatik Professor an der Duke University).

Exkurs: Industrial Internet und Industrie 4.0

Es sollen nun auch noch kurz die verwandten Begriffe Cyber-Physical Systems, Industrie 4.0 und Industrial Internet erläutert werden. Cyber-Physical Systems ist im Wesentlichen die akademische Übersetzung des Begriffs Internet der Dinge, also die Verbindung von physischen Dingen mit dem „Cyberspace“, dem Datenraum des Internets.

Industrial Internet bezeichnet die Anwendung von IoT Technologien im Bereich der Industrie wobei mit Industrie in diesem Zusammenhang nicht nur die industrielle Fertigung gemeint ist sondern alles was nicht in den Konsumbereich fällt. Somit fallen neben herkömmlicher Automatisierungstechnik auch die Bereiche Medizintechnik, Gebäudetechnik, Smart Grid, Logistik, usw. unter Industrial Internet. Der Begriff ist somit nicht direkt mit dem in Deutschland geprägten Industrie 4.0 vergleichbar, welcher einen wesentlich engeren Bezug zur industriellen Produktion, insbesondere der Optimierung des Fertigungsprozesses bis zur theoretischen Losgröße 1 mit Hilfe von neuen Technologien, hat, quasi die 4. Industrielle Revolution. Generell leidet der Begriff Industrie 4.0 darunter, stark politisch vereinnahmt zu sein und hauptsächlich Arbeitsgruppen und viel Papier zu produzieren. Einen pragmatischeren Weg geht das US-lastige, aber mittlerweile international besetzte Industrial Internet Consortium, welches konkret an Testbeds und Quasi-Standards arbeitet. In letzter Zeit ist allerdings eine Annäherung zwischen den Industrie 4.0 und IIC Arbeitsgruppen wahrnehmbar.

Um auch gleich ein mögliches Missverständnis auszuräumen: Industrial Internet, bzw. Industrie 4.0 bedeutet nicht, jetzt quasi die gesamte Fertigung „ans Internet zu hängen“. Vielmehr ist die Nutzung von Internet-Technologien gemeint, die sehr wohl auch in einem vom offenen Internet möglichst gut abgesicherten Firmennetz erfolgen kann. Ziel ist dabei eine verbesserte Integration der Automatisierungsebene und des entstehenden Produktes untereinander, sowie mit den IT Systemen (z. B. ERP und CRM) des Unternehmens über den gesamten Lebenszyklus des Produktes hinweg.

2. Chancen und Herausforderungen für österreichische Unternehmen

Betrachtet man diverse Marktstudien zum Thema IoT wird man zwangsläufig mit gigantischen Fantaziezahlen überschüttet. Je nach Studie erwartet man für 2020 zwischen 5 und 50 Milliarden „connected devices“. In wie weit sich diese Prognosen bewahrheiten werden sei dahingestellt. Was jedoch mit Sicherheit gesagt werden kann ist, dass die Konzepte hinter IoT bleiben werden, auch wenn der Begriff IoT in ein paar Jahren vielleicht durch einen neuen Marketingbegriff abgelöst werden wird. Es lohnt sich also, sich schon jetzt mit den Grundlagen des IoT vertraut zu machen.

Aus technischer Sicht ist zunächst zu erwähnen, dass alle für das IoT notwendigen Technologien bereits seit einiger Zeit verfügbar sind. Das IoT ist somit kein vornehmlich technisches Problem mehr. Die eigentliche Herausforderung die das IoT mit sich bringt ist die vollständige Umstrukturierung von Geschäftsmodellen und Geschäftsprozessen, welche Unternehmen meistern müssen.

Neue Geschäftsmodelle – ein Praxisbeispiel

Ein Beispiel wie ein solcher Transformationsprozess eines Geschäftsmodells aussehen kann liefert ein österreichisches Unternehmen, bekannt vor allem für Seifen- und Handtuchspender im Sanitärbereich. Das Unternehmen hat damit begonnen, Seifen- und Papierspender mit Sensoren und Funkmodulen auszustatten, welche Füllstands- und Nutzungsdaten über eine Basisstation an einen Server des Unternehmens senden. Dies hilft dem lokalen Facility Management schon einmal dafür zu sorgen, dass leere Seifen, bzw. Papierspender der Vergangenheit angehören. In Kombination mit einem ebenso eingebundenen Besucherzähler lassen sich weiters interessante Daten ableiten. So weiß das Unternehmen mittels einer recht großen Datenbasis mittlerweile sehr genau, wie viel ein Toilettenbesuch im Endeffekt kostet. Dies wiederum ermöglicht eine komplette Umstellung des Geschäftsmodells. Anstatt Handtücher und Seife zu verkaufen, und sich dabei mit möglichen billigeren Alternativenbietern konkurrieren zu müssen, verrechnet das Unternehmen nur mehr die Anzahl der Toilettenbesuche. Dies ist einerseits für den Kunden bequemer, da einfacher zu kalkulieren, und der Kunde sich nicht mehr um die rechtzeitige Nachbestellung des Verbrauchsmaterials kümmern muss. Andererseits verschafft sich das Unternehmen natürlich einen Vorteil gegenüber möglichen Konkurrenten, die diese Art der Kundenbetreuung und Kundenbindung gar nicht bieten können.

Vom Produzenten zum Dienstleister

Im gerade angeführten Beispiel ist eine deutliche Verschiebung des Geschäftsmodells vom Produktverkauf (Seife, Papiertücher) zur Dienstleistung (Toilettenbesuch) zu erkennen. Diese Verschiebung vom Produkt zur Dienstleistung ist bezeichnend für das Internet der Dinge. Besonders hervorgehoben werden muss in diesem Zusammenhang die Bedeutung von Software. Vom der Firmware im Seifenspender, über die Basisstation, bis hin zur Unternehmenssoftware welche die gesamte Logistik von der automatischen Nachbestellung bis zur Lieferung steuert, sowie die anfallenden Daten auswertet (Business Intelligence), Software überall.

Unternehmen die das Internet der Dinge in vollem Ausmaß zum wirtschaftlichen Vorteil nutzen wollen müssen im Endeffekt zu Softwareunternehmen werden. Speziell für Unternehmen welche Software bis jetzt eher als „lästiges Beiwerk“ betrachtet haben, ist radikales Umdenken angesagt. Siehe dazu auch Marc Andreessen's bekannten Artikel im Wall Street Journal: "Why Software is Eating The World".

3. Technische Aspekte

Das Internet der Dinge wird gebildet aus "Dingen", Kommunikationsinfrastruktur und Computern. „Dinge“ sind vernetzte „Smarte Produkte“ und andere Gegenstände, welche ein Computersystem (Microcontroller), Sensoren, Aktoren und Software mit Kommunikationstechnik kombinieren. Weiters benötigt man eine Kommunikationsinfrastruktur, welche die Dinge mit dem Internet verbindet. Das beinhaltet energiesparende drahtlose PANs (Personal Area Networks) wie z. B. ZigBee, Thread oder Bluetooth, lokale Netzwerke (WLAN, Ethernet), bis hin zu weitläufigen Netzwerken (ADSL, UMTS, 4G, LoRa).

Schlussendlich benötigt man leistungsfähige Computer, um alle angebundenen Dinge zu verwalten, sowie um die anfallenden Daten zu verarbeiten. Gerade erst durch die Verarbeitung aller in massiver Form anfallenden Daten – Stichwort „Big Data“ – durch neuartige Datenerfassungs- und Analyse-Software ergeben sich neue Arten der Wertschöpfung, bzw. neue Geschäftsideen.

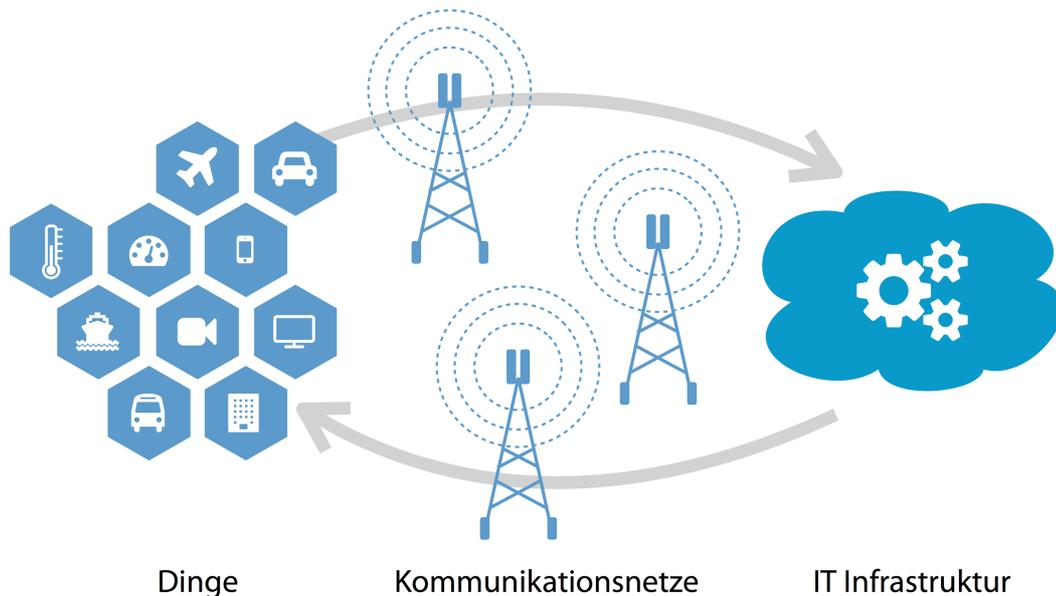


Abbildung 1: Bausteine für das Internet der Dinge

Technologien

In den letzten Jahren entstand eine Vielzahl neuer Technologien welche verschiedene Aspekte, bzw. verschiedene Ebenen des IoT abdecken. Dieser „IoT Technology Stack“ wird im Folgenden vorgestellt. Eine typische Referenzarchitektur für ein IoT System besteht aus folgenden Komponenten:

Sensoren, bzw. Aktoren welche z. B. über ein drahtloses Sensornetzwerk mit einem IoT Gateway (auch Basisstation genannt) verbunden sind. Dieser IoT Gateway hat die Aufgabe, mit den angeschlossenen Sensoren, bzw. Aktoren zu kommunizieren, und in weiterer Folge die Verbindung zur nächst höheren Ebene, oft als „Cloud“ bezeichnet, herzustellen. In der Cloud wiederum laufen all jene Applikationen, welche die anfallenden Daten auswerten und

in die Geschäftsprozesse des Unternehmens integrieren. Ob diese Applikationen jetzt auf einem „public“ Cloud Service im Internet laufen, oder im privaten Rechenzentrum eines Unternehmens ist hier zweitrangig, da die Kommunikation in beiden Fällen gleich abläuft. Security-Aspekte sind aber unbedingt zu berücksichtigen. Diese Architektur ist natürlich nicht in Stein gemeißelt. So können die Rollen von IoT Gateway und Sensor/Aktor vom selben Gerät übernommen werden. Der Kommunikationsfluss ist natürlich in beide Richtungen möglich. Dinge können Informationen aus der Cloud beziehen und auch lokal untereinander, ohne Umweg über die Cloud, kommunizieren.

Unternehmens-IT, Cloud, Big Data	Intel Xeon, SPARC	Linux, Solaris, Windows Server
Internet (LAN, WAN)	Ethernet, Wi-Fi, xDSL, UMTS/HSPA/LTE	MQTT, HTTP, REST, SOAP, Web Services
IoT Gateway	ARM 9, Cortex A8/9, Intel Quark/Atom	Linux, Windows Embedded
Sensor Netzwerk	IEEE 802.15.4, Wi-Fi, Bluetooth, EnOcean	ZigBee, Z-Wave, 6LoWPAN, CoAP, LWM2M, Thread
Sensor, Aktor, "Thing"	Atmel AVR ARM Cortex M	Contiki, Tiny OS, RIOT, mbed

Abbildung 2: IoT Technology Stack: Technologieebene, Hardware und Software/Protokolle

Dinge, Sensoren und Aktoren

Beginnen wir bei den kleinsten Geräten, typischerweise Sensoren und Aktoren, welche über ein sogenanntes Sensornetzwerk miteinander, sowie mit einem IoT Gateway (Basisstation), verbunden sind. Diese Devices basieren üblicherweise auf einem kleinen 8, 16 oder 32-bit Microcontroller wie einem Atmel AVR oder einem ARM Cortex M. Zur Vernetzung kommt ein typischerweise auf IEEE 802.15.4-basiertes Funknetzwerk zum Einsatz. Für diese Devices wurden eine Reihe von kleinen, spezialisierten Betriebssystemen entwickelt, wie z. B. Contiki, Tiny OS, RIOT oder mbed. Diesen Betriebssystemen ist gemeinsam, dass sie von Grund auf für Vernetzung, als auch Energieeffizienz ausgelegt sind. 6LoWPAN und CoAP scheinen sich hier als Standard-Netzwerkprotokolle zu etablieren, da diese Protokolle offen und frei verfügbar sind. Technologien wie ZigBee, Z-Wave, Thread, Bluetooth, EnOcean, aber auch schon Wi-Fi kommen hier ebenfalls zum Einsatz. Im Bereich der Wide Area Netzwerke gewinnt LoRa zunehmend an Bedeutung. Gerade im Industriebereich sind hier aber auch Feldbussysteme anzutreffen, OPC-UA und DDS sind hier ebenso von Bedeutung. Beispiele solche Devices sind z. B. Funksensoren zur Temperatur-, Luftfeuchtigkeits- und Helligkeitsmessung, oder die bekannten programmierbaren Philips Hue Lampen, welche über ein ZigBee Funknetzwerk kommunizieren. Auch die angesprochenen vernetzten Seifen- und Handtuchspender gehören dazu.

IoT Gateway als Vermittler

Der IoT Gateway stellt das Bindeglied zwischen den kleinen Devices, den Sensornetzwerken und der Internet-Welt dar. IoT Gateways sind oft Linux-basierte Geräte mit leistungsfähigen ARM Cortex A oder Intel Quark/Atom CPUs. Verschiedene Netzwerkschnittstellen sorgen für Connectivity, ein UMTS/4 G Modul für mobilen Internetzugang kann integriert sein. Neben Ihrer Funktion als Übersetzer und Vermittler zwischen Sensor und Cloud/IT-Welt können Gateways ebenso komplexere Applikationen ausführen. Beispiele sind die Filterung, Vorverarbeitung und Protokollierung von Sensordaten, (unkritische) Steuerungsaufgaben, Alarmierungen per SMS oder E-Mail, Visualisierungen von Anlagenzuständen über eine Webseite, usw. Schlussendlich ist es jedoch meistens das Ziel, die erfassten Daten an einen Server weiterzusenden, wo sie dann in einer Datenbank gespeichert, mit anderen Daten kombiniert und analysiert werden. Zur Kommunikation zwischen Gateway und Server haben sich im Wesentlichen zwei Protokolle etabliert. Zunächst einmal werden HTTP/REST Web Services verwendet, die sich im Internet-Bereich weitgehend als Standard etabliert haben. Ebenso sind HTTP/SOAP Web Services möglich, speziell im Bereich der Unternehmens IT wo sie weite Verbreitung gefunden haben. Ausgezeichnet für das Internet der Dinge eignet sich allerdings das MQTT Protokoll. Obwohl bereits seit 1999 entwickelt erfreut es sich gerade erst jetzt großer Beliebtheit. Ein Grund dafür ist einerseits der geringe Protokoll-Overhead, speziell im Vergleich zu HTTP. Andererseits ist MQTT sehr robust, was gerade im Fall schlechter Verbindungen (z. B. mobiles Internet) ein Vorteil ist. MQTT ist auf die Übertragung von Telemetriedaten optimiert, was sich auch im Namen – Message Queuing Telemetry Transport – widerspiegelt. Eine spezielle Eigenschaft von MQTT ist, dass Sender und Empfänger einer Nachricht nicht direkt miteinander kommunizieren. Die Kommunikation läuft immer über einen sogenannten Broker, nach dem Publish-Subscribe Verfahren. Das heißt, ein Gerät oder eine Applikation welche Nachrichten senden möchte, sendet diese unter einem sogenannten „Topic“, ein hierarchisch aufgebauter Name. Geräte, bzw. Applikationen welche Daten empfangen möchten geben jene Topics an, zu denen sie Nachrichten empfangen möchten. Es ist dann Aufgabe des Brokers, alle Nachrichten den jeweils interessierten Empfängern zuzustellen. Jeder Teilnehmer (im MQTT Jargon „Client“) kann gleichzeitig Sender und Empfänger sein. Der MQTT Broker ist für die Authentifizierung und Autorisierung der Clients verantwortlich, und die Kommunikation erfolgt üblicherweise verschlüsselt (SSL/TLS), so dass auch ein hohes Maß an Datensicherheit erreicht werden kann. Ein wichtiger Grund für die Beliebtheit von MQTT ist die Verfügbarkeit qualitativ hochwertiger Open Source Implementierungen für eine Vielzahl von Plattformen.

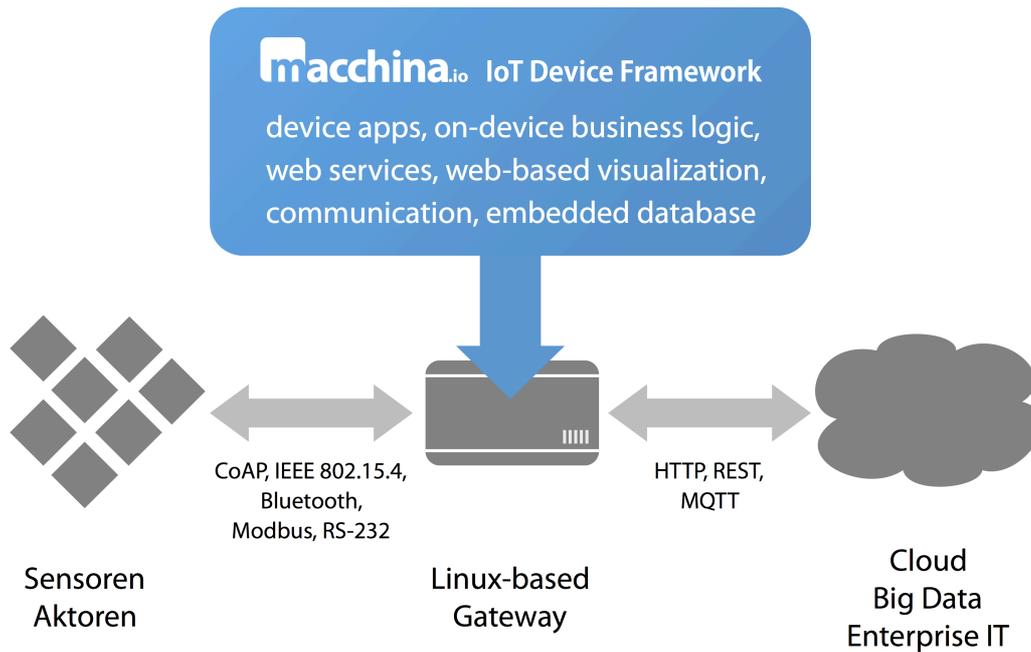


Abbildung 3: Der IoT Gateway als Vermittler zwischen Sensor und Cloud.

Exkurs: Einsatz von Gateways zum sicheren Fernzugriff und zur Fernwartung

Neben dem Sammeln, Verarbeiten und Weiterleiten von Sensordaten werden IoT Gateways auch zum sicheren Fernzugriff eingesetzt. Der oft bereits vorhandene Web Server eines IoT Gateways bietet beste Voraussetzungen zur Implementierung einer Fernzugriffs-, bzw. Fernwartungslösung, muss doch nur eine Möglichkeit geschaffen werden, auf ebendiesen Web Server aus der Ferne zugreifen zu können. Natürlich auch dann, wenn das Gerät selbst über das Internet nicht direkt erreichbar ist, was in den allermeisten Fällen der Fall ist, und aus Sicherheitsgründen auch sein sollte. Immer noch viel zu oft wird eine Kombination aus Port Forwarding am Router, sowie Dynamic DNS eingesetzt um Fernzugriff zu ermöglichen. Allerdings ist dies aus sicherheitstechnischer Sicht höchst problematisch. Vor einigen Jahren hat ein bekannter Hersteller von Heizungen höchst unliebsame Erfahrungen mit so einer Implementierung machen müssen. Wesentlich besser ist der Einsatz eines VPN. Ganz unproblematisch ist aber auch diese Lösung nicht. Zunächst einmal ist die benötigte Server-Infrastruktur recht aufwändig. Dann muss dafür Sorge getragen werden, dass innerhalb des VPNs die einzelnen Geräte trotzdem voneinander abgeschottet werden, ansonsten könnte die VPN Anbindung eines einzelnen Gerätes missbraucht werden, um in andere Geräte einzudringen. Schlussendlich ist ein VPN nicht gut geeignet, auch Endkunden den Fernzugriff auf ihre eigenen Geräte zu ermöglichen. Um neben dem Hersteller auch Endkunden oder Service-Partnern den sicheren Fernzugriff auf Geräte zu ermöglichen gibt es Lösungen wie z. B. *my-devices.net*.

Internet

Ein wesentlicher Unterschied zwischen IoT und M2M ist die Verwendung von Internet Technologien und offenen Protokollen für die Kommunikation im IoT, während bei M2M vorwiegend proprietäre Technologien und Protokolle zum Einsatz kommen. Als Datenformat hat sich JSON gegenüber XML weitgehend durchgesetzt und kommt sowohl mit MQTT, als auch HTTP/REST-basierten Web Services zum Einsatz.

Cloud, Unternehmens-IT und "Big Data"

Die bei den meisten IoT Anwendungen anfallenden Datenmengen erfordern eine leistungsfähige Computerinfrastruktur zur zeitnahen Weiterverarbeitung, um daraus einen wirtschaftlichen Vorteil zu erzielen. Neben einer Analyse der anfallenden Daten mit "Big Data" Technologien wie Hadoop, Spark oder Kafka ist auch deren Weiterleitung in Unternehmensapplikationen (ERP, CRM, etc.) erforderlich.

4. Einstieg ins Internet der Dinge mit *macchina.io*

Wie kann nun ein schneller Einstieg ins Internet der Dinge erfolgen? Dank kostengünstiger Hardware wie Raspberry Pi und frei verfügbarer Open Source Software ist für experimentier- und spielfreudige Techniker ein Einstieg recht schnell möglich. So bietet z. B. das deutsche Unternehmen Tinkerforge diverse Sensoren und Aktoren an, die über USB einfach mit einem PC oder Kleincomputer, wie z. B. einem Raspberry Pi oder BeagleBone, der als IoT Gateway fungiert, verbunden werden können. Einfach zu nutzende Programmierschnittstellen sind mit dabei.



Abbildung 4: Aufbau von *macchina.io*, einer Software Plattform für IoT Gateways

Als Software für den IoT Gateway bietet sich *macchina.io*, ein unter österreichischer Führung entwickeltes Open Source Projekt an. Damit kann die Software für Linux-basierte IoT Gateways recht einfach in der Programmiersprache JavaScript entwickelt werden. Performance-kritischer Code, sowie die low-level Anbindung von Geräten, neuen Netzwerkprotokollen, usw. kann auch in C++ realisiert werden. Für verschiedene Sensoren (z. B. Tinkerforge), Netzwerkprotokolle (MQTT, HTTP) und Dienste (z. B. Versand von SMS) sind vorgefertigte Schnittstellen und Software-Module vorhanden. Ein besonderes Highlight ist der „Playground“, ein Web-basierter Editor für JavaScript. Damit können schnell ein paar Zeilen JavaScript erstellt, und direkt auf dem Gateway ausgeführt werden. Erste

Erfolgslebnisse sind so schnell möglich. Als Beispiel sei das „Hello, world!“ Programm für das Internet der Dinge genannt: In regelmäßigen Zeitabständen wird mittels Temperatursensor die aktuelle Temperatur gemessen und über MQTT an einen Broker übermittelt. Dies lässt sich in weniger als 10 Zeilen JavaScript Code umsetzen. Mit nur wenigen Zeilen mehr kann auch eine Alarmmeldung per SMS gesendet werden, wenn die Temperatur einen Schwellwert überschreitet, z. B. über das Twilio Web Service. Natürlich sind richtige IoT Applikationen um einiges komplexer. Allerdings ermöglicht schon eine einfache Applikation das Kennenlernen aller wesentlichen Technologien.

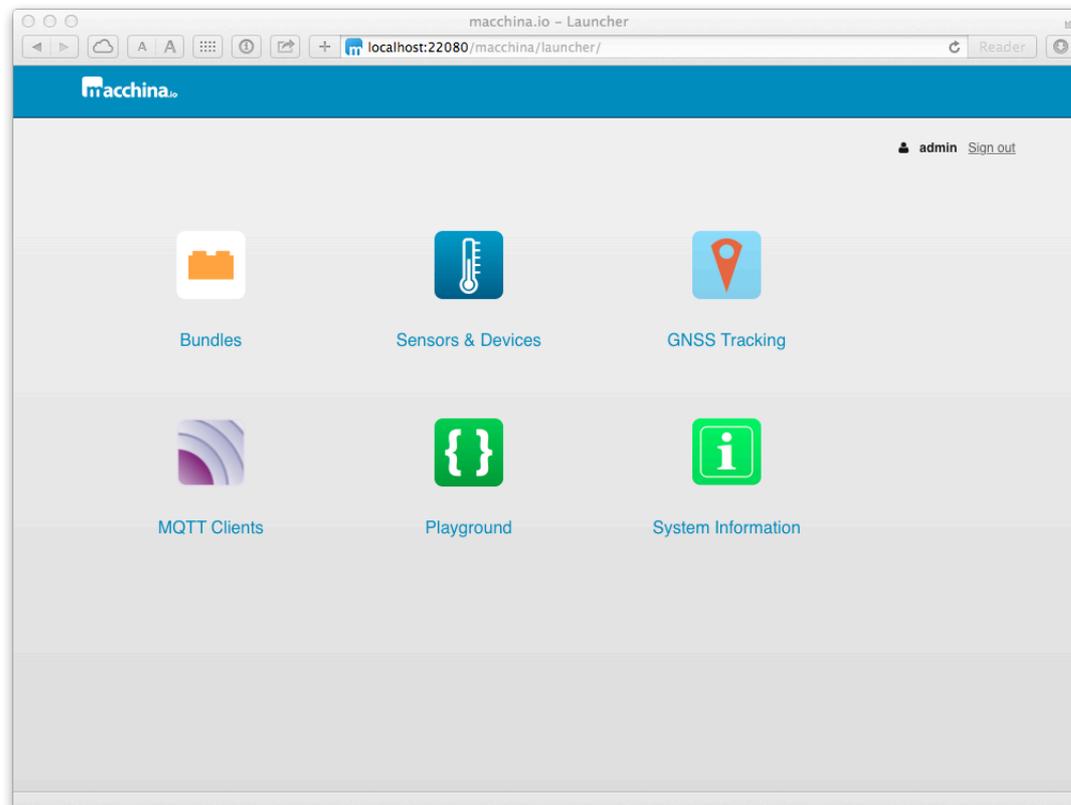


Abbildung 5: Web Oberfläche von macchina.io

Zusammenfassend ist zu sagen, dass das Internet der Dinge keine ferne Zukunftsvision ist, sondern von den ersten Unternehmen bereits gewinnbringend eingesetzt wird. Dazu ist neben der Einführung neuer Technologien jedoch vor allem ein Umdenken auf Geschäftsprozessebene erforderlich. Der Einstieg in die neuen Technologien ist dank kostengünstiger Hardware und Open Source Software recht einfach zu schaffen.



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 4.0 International Lizenz.