The IoT Dictionary

ADD SECURE

Introduction

A new field like the Internet of Things necessarily introduces a whole slew of new expressions and acronyms. You're probably already familiar with some of them, while some merit a further explanation. We've done our best to collect the most relevant expressions, as well as an explanation of what role they play in the IoT. This means that even though some expressions, like malware or firewall, are probably well known by you already, might have new uses or important connotations within the world of IoT.

Whether you read this dictionary from cover to cover, or use it as an encyclopedia when you run into a particularly consonant heavy acronym, I hope you'll find the information contained here useful. If a word is missing, or you have other questions, you're more than welcome to contact us directly. IoT is an enormous field, so it would never be possible to create a full picture through one ebook.

With that, I wish you happy reading.
Per Christian Foss

Contents

ADDSECURE

A

AI

Artificial intelligence (AI) has recently gone from being science fiction, to relevant, existing technology. Through algorithms that allow machine learning, computers can learn even complicated tasks we wouldn't be able to program from scratch. This is important to organize and find meaning in the enormous data sets available through the IoT (see Big Data).

Actuator

Actuators are the components in an electronic device that converts electrical signals into output like light, movement or other functions. They're often spoken of as the counterpart to sensors.

API

An Application Programming Interface (API) is, as the name suggests, a programming interface to easily connect a software or service to another one. To take an example, Facebook's API lets other websites use their login and user information, without having to program this from the bottom up. API's are an important part of the IoT, as it lets you incorporate crucial information from IoT devices into your own IT systems.

APN

An Access Point Name (APN) identifies the access point for a gateway between the mobile network and the internet. This means mobile devices can easily connect to the internet through the mobile network.

B

Beacons

Beacons are little bluetooth transmitters placed around to give you information or ads based on where you're at geographically. This information or advertising will usually appear on your smartphone, and can even adjust itself based on what the sender knows about you.

Big Data

Big Data are data sets so large that traditional ways to process or analyze them don't suffice. With connected devices everywhere around us, the amount of information they gather is radically increased, meaning Big Data is a huge part of the IoT. Luckily, new technology doesn't just let us collect more data, but also process it more effectively. The amount of data needed to count as Big has increased proportionally with technology's ability to gather and store it. Where we used to talk about gigabytes of information, we'd now rather talk about exabytes (1,000,000,000,000 MB)

Botnet

A botnet is a network of connected machines or devices that have been hijacked for other purposes. Through malware, hackers can access huge amounts of processing power by combining these so called zombie machines into larger networks, and use them to (for example) deliver spam email or overload other networks/servers with traffic from every zombie at once. Devices could very well be part of a botnet even though you still use them, but they'll often be a lot slower since they use so much power on other processes. Plenty of botnets have already been discovered on the IoT.

C

Capacity

Capacity refers to the amount of users and devices a network is able to handle.

Cloud

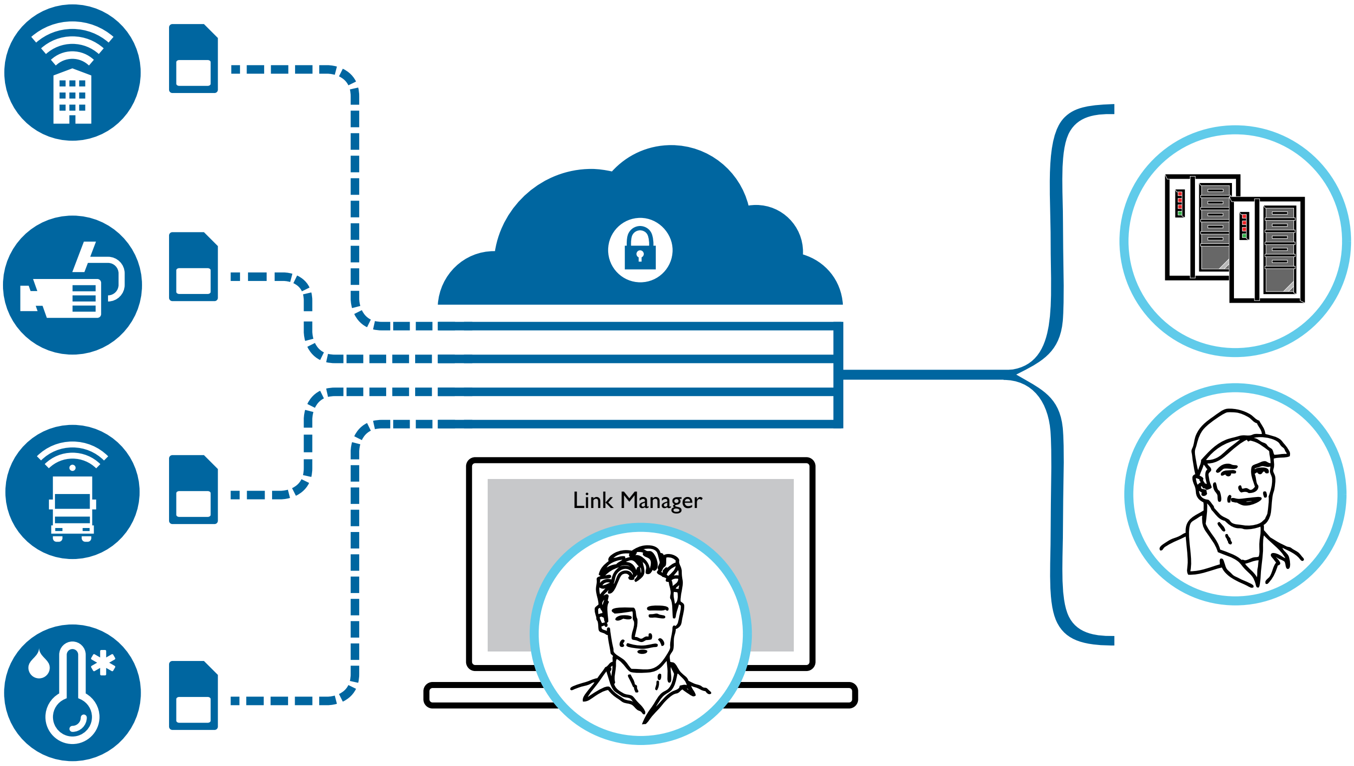
If you use cloud services, that means you're letting external servers take care of actions like storing and processing data, rather than doing it locally on your computer or device. This frees up a lot of storage and processing power for each unit, making the information easier for you to access, and is even safer as long as the cloud service is encrypted.

Connected car

A connected car, or more generally, a connected vehicle, is a vehicle connected to the internet, often with its own local area network (LAN). Connected cars are already widespread, and the connection is often used for things like the car's entertainment system, navigation, remote controlled functions and so on. In the future, it may be used to coordinate self driving cars.

Coverage

Coverage is the geographical area a network signal can reach. This may be affected both by the devices transmitting them (like base stations), and the physical environment itself.


Link Manager

D-E

DoS/DDoS

A denial-of-service attack (DoS) is a common way of attack for hackers wanting to disable a system. This could be done by for example sending little programs ordered to copy themselves infinitely, until the processor can't keep up anymore. Another version is distributed denial-of-service attacks (DDoS). This means using a botnet to send so much data that it exceeds the victim's bandwidth, making the website or service crash. The common denominator is forcing a system to perform such massive and challenging tasks that it breaks down.

eHealth

eHealth is the pretty all-encompassing term for a health service supported by electronic and digital solutions. IoT will by all likelihood have a huge effect on this sector, through things like automatically shared and updated health journals, and wearables that can discover disease and health issues.

Encryption

Encryption is a way of protecting data by using an algorithm to transform the data into an essentially undecipherable "language", requiring a "key" to decrypt. Encryption is already a common way of protecting sensitive data online, and will continue being highly important within the IoT.

eUICC

An Embedded Universal Integrated Circuit Card, or eUICC, is a new type of integrated SIM card that allows you to switch mobile operators without physically changing the SIM. Everything is done over the air (OTA).

F-H

Firewall

A firewall is a barrier that protects a network from unwanted traffic. An IoT firewall has somewhat different demands than a standard firewall on a computer. The latter is often too big for the more limited IoT devices, and also has a tendency to filter out other things than what's most strictly needed for the IoT. This is why you need to adapt the kind of firewall you're using, depending on what it's protecting.

Hacking

Hacking refers to exploiting weaknesses in digital systems to gain access you're not meant to have. This could lead to major problems, and be especially dangerous now that more and more devices are being connected to the internet. Nuclear power plants, sensitive user data, life supporting equipment in hospitals – all this could easily be accessed by hackers if security isn't made a top priority.

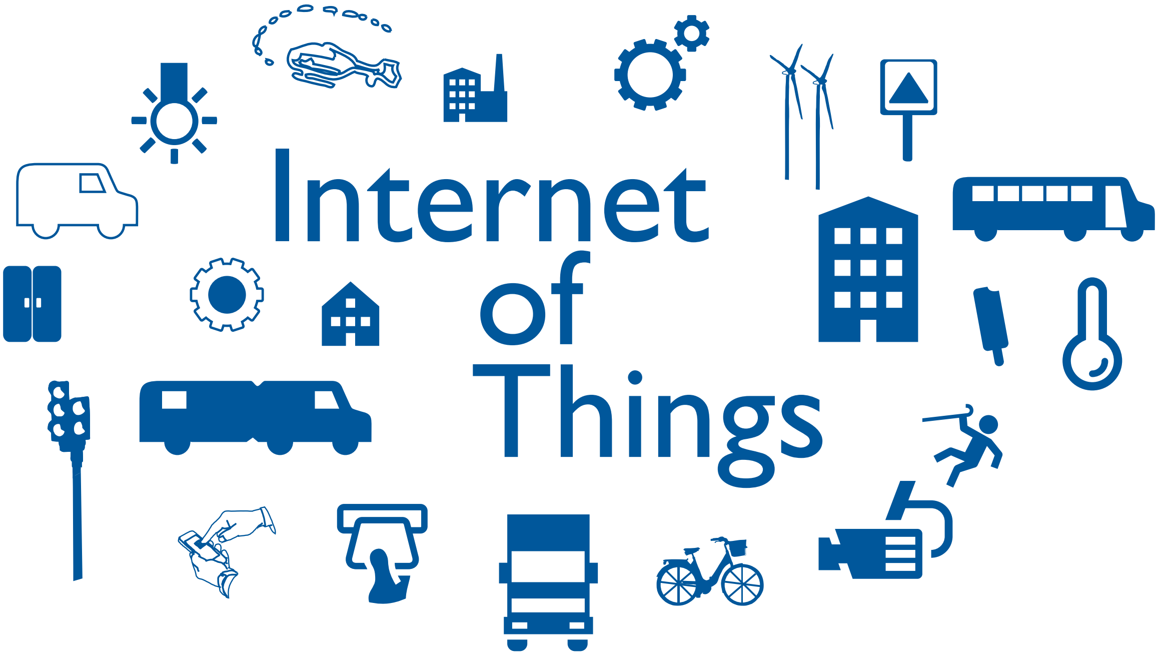
I

IAM

Identity & Access Management (IAM) is a set of tools and routines that make sure only the people meant to have access to a network gain access, while removing those who aren't.

IoT

We can't get around a definition of the main theme itself: the Internet of Things. This is essentially an expanded internet, where all kinds of devices are connected and may exchange information, as opposed to the internet of today, which mainly allows people to do the same thing through browsers.



L

LAN

A Local Area Network is a geographically limited network, often just for a single building.

LPWA

A Low-Power Wide-Area Network (LPWA) is a type of wireless communication network that works really well for the IoT. It has a wider range, but doesn't have the same speed as for example 4G for cell phones. The communication modules used for LPWA are low cost and consume little power, making LPWA ideal for a range of IoT uses. There are several competing standards, like NB-IoT and LoRa.

M

M2M

For many, M2M communication might be a more familiar expression than IoT, and they're often used interchangeably. M2M stands for machine-to-machine communication, and refers to connected devices communicating directly, without a human middleman. We can say that M2M is what allows for the IoT to work, while IoT itself is a wider term, encompassing M2M networks, but also the ecosystems around them. IoT is what brings the physical and the digital world together.

Malware

Malware, or malicious software, is a catch all term for software that consciously tries to exploit or destroy your devices. Examples are computer worms, keyloggers or adware. There's plenty of malware in the IoT, but might be harder to discover as the IoT devices tend to have such limited functions that they're not visibly affected.

Managed Connectivity

Managed connectivity is a term for solutions that allows for monitoring, controlling and self-service within IoT communication.

M

Mesh

Mesh is a type of network that's different from (for example) Wi-Fi, in that a mesh network is built from many small, interconnected nodes, rather than all passing through one point, i.e. a router. As every node in a true mesh system is connected to every other node, it's more expensive, yet a lot more secure, as there's always many connections left even though one were to fail. There are also partial mesh networks, where many, though not all, nodes are connected.

MNO

A Mobile Network Provider (MNO) owns and controls all necessary elements to offer mobile services, including base stations, radio frequencies and core networks.

Multi factor authentication

Multi Factor Authentication, commonly two factor authentication, is a security measure that's especially used for processes involving sensitive data. A good example is having to input a code sent to your cell phone as well as your normal password. By involving two or more factors, it's harder for hackers to log in to i.e. your online bank account, or your IoT network.

O-R

OpenVPN

OpenVPN is freeware that helps you easily set up virtual private networks (VPN).

PKI

Public Key Infrastructure (PKI) is a way to ensure that information is transferred securely, in cases where normal password verification won't suffice. It operates with both a public and a private key, which together confirms that whoever asks for access is who he claims to be.

Protocol

A communication protocol is a set of rules that determine how devices communicate. There's a whole number of these, like Bluetooth, Wi-Fi, or the IoT centered ZigBee. IoT is in such an early phase that there's not yet a common standard protocol, but many competing ones that don't always work together.

RFID

Radio Frequency Identification (RFID) is a system that works by having small tags communicate over very short distances through radio signals. These are commonly used for tracking, identification, verification, payment, or burglary alarms.

S

Sensor

As the IoT is largely focused on connecting our physical environment to the internet, sensors are incredibly important. These are the components that “sense” the world around them, through registering for example light, temperature or humidity, and converting it into data. Through M2M communication, smart devices may automatically respond to the environment, with no human input.

Server

A server is a machine or a computer program that performs services for other machines (typically computers or cell phones), called clients. Typical services are storage or email functionality, freeing up space on the more user oriented devices. An IoT network is typically made up of sensors and actuators being controlled through a server.

Smart city

A smart city is the expression we use for a city where IoT is thoroughly integrated with everything from traffic to schools to hospitals. By using this technology, we may streamline a lot of processes through automation, and create better and more sustainable solutions for the inhabitants.

T

Two-step verification

Also known as a two-step confirmation, is an added safety feature often applied when sensitive data is involved. The two-step verification usually means that two different passwords is required to gain access, where one of the passwords are single use, and sent to a device, for example, a mobile phone. The added step makes it more difficult for unauthorized persons to gain access to an online bank account or an IoT network.

V-W

VPN

Virtual Private Networks (VPN) is a closed, encrypted connection (a tunnel) on the internet. To gain access you have to go through an authentication process. VPN is a much more secure type of network than the open internet, which makes it ideal for IoT purposes.

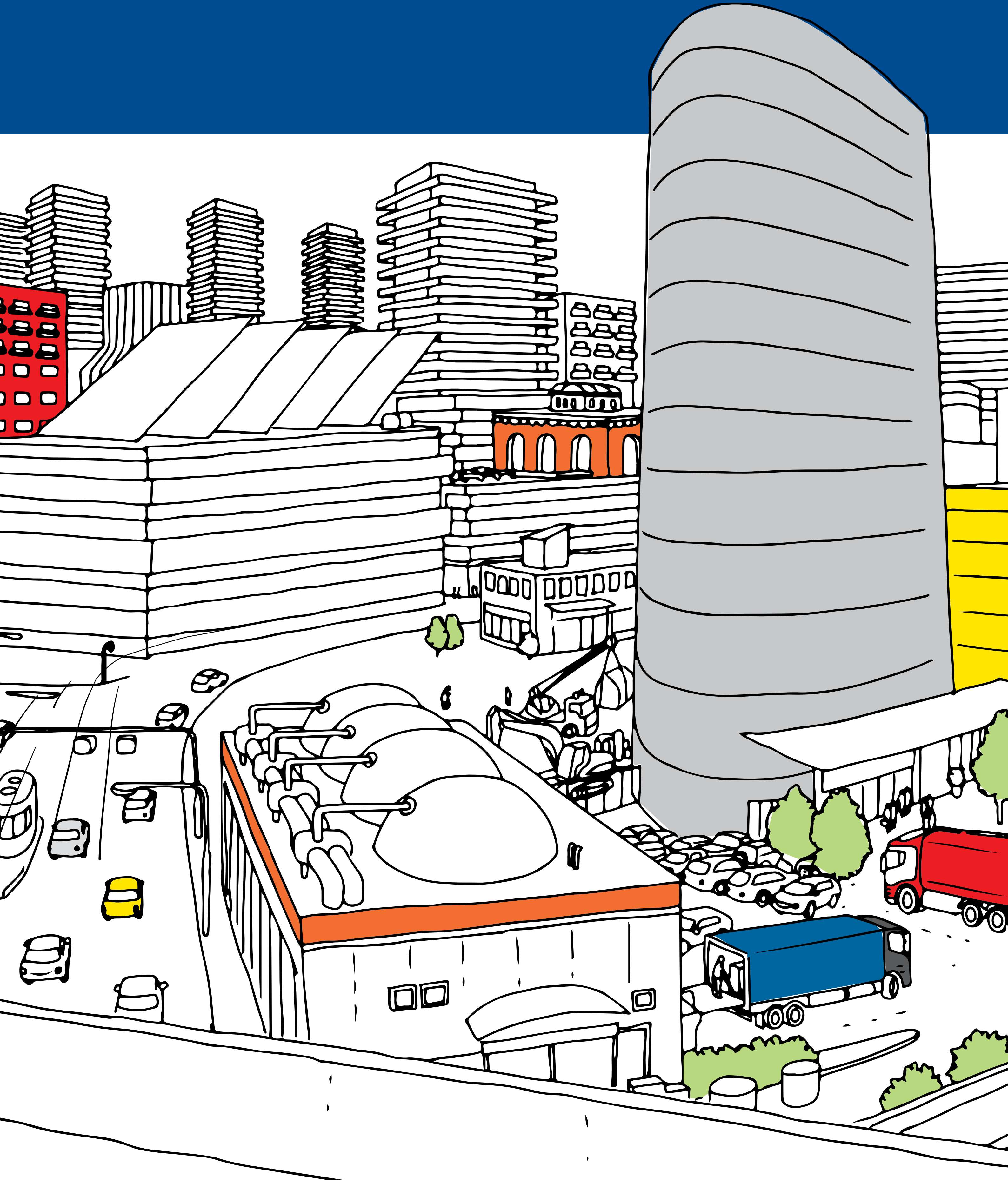
WAN

Wide-Area Network (WAN) is simply a network that stretches over a wide geographical area. The internet itself could be considered a WAN, but it's so enormous that it's usually better to speak of it as a thing of its own. WAN stands in contrast to geographically limited Local Area Networks (LAN).

Wearables

Wearables (or wearable technology) is technology you can wear. This is going to be more common as the IoT grows, but one might quite reasonably consider traditional devices like digital watches or hearing aids as wearables. Others claim the device has to be connected to the internet to count as a wearable. Activity trackers and various health sensors that communicate their findings over the internet are good examples of these.

ADDSECURE



Would you like more information about IoT or simple and secure communication for data transfers?

Get in touch with one of
our IoT advicers

I wish to get in touch

ADDSECURE®
Have a safe day