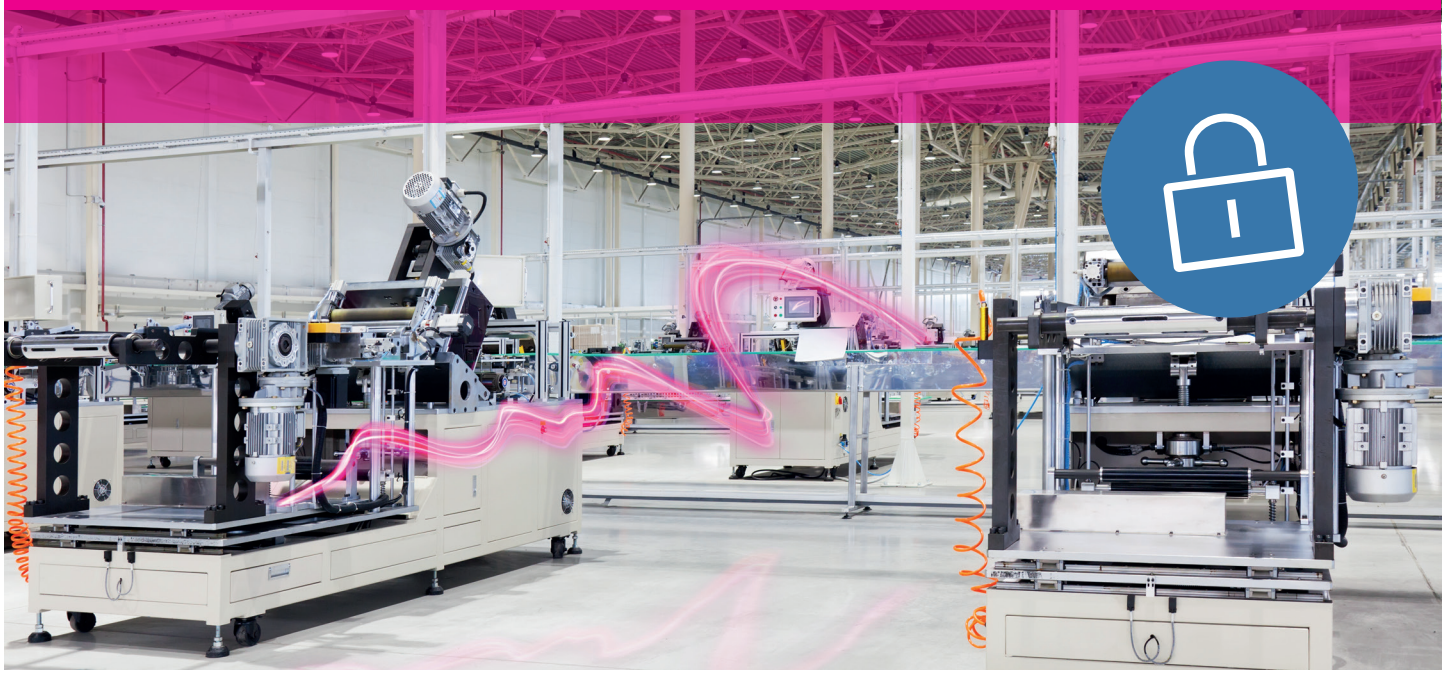
LIFE IS FOR SHARING.

THE CLOUD OF THINGS – SECURITY FOR YOUR DATA



When intelligent networking connects people and industrial processes and when information and communication technologies are interlinked, that's Industry 4.0. The Internet of Things is a basic requirement for smooth operation. In order for companies to take full advantage of the benefits of a cloud-based IoT platform and to future-proof their business models, corporate, customer and sensor data must be protected as well as possible. As the role of security continues to increase, you need the most important facts, which we present here.

IS ENCRYPTION REALLY NECESSARY?

Of course, locking the door to your house by no means ensures that a break-in will not occur – but the more difficult you make it to enter, the better the chances that possible intruders will give up on their plans. This is also true for your data. The better you protect your data, the lower the risk of it falling into the wrong hands.

Data encryption is similar. Unfortunately, it still does not guarantee that criminals will not find a way to access your data. What's important here is that even in such a case, encryption makes it impossible for the criminal to read the data. Data encryption also hinders alterations to the data and the dissemination of false or counterfeit data. Even in the worst case scenario, your system and your data are protected.

WHY USE THE DEUTSCHE TELEKOM CLOUD OF THINGS? YOUR BENEFITS AT A GLANCE.

- Standardized security and data privacy concepts with Deutsche Telekom's own PSA procedure (Privacy and Security Assessment)
- The most advanced data centers in Germany – in accordance with the highest Deutsche Telekom security standards
- Multi-tenancy to segregate customer data into completely separate data areas
- Approval by Deutsche Telekom security experts before each release
- Inspection and certification of IoT devices connected with the Cloud of Things

THE SECURITY OF YOUR DATA HAS TOP PRIORITY – OUR MEASURES MAKE THE CLOUD OF THINGS EVEN MORE SECURE.

THE HIGHEST SECURITY STANDARDS ARE A MUST!

Potential targets for cyber attacks are most often network connections between the customer's browser and the Cloud of Things. The radio links between devices are also at risk. These provide a variety of starting points for espionage or attempts at sabotage – with severe consequences for companies. In addition to spying and the manipulation of data, a product's image or that of an entire company can be destroyed. That's why the security of your data is extremely important.

With this in mind, Deutsche Telekom has given top priority to the security of its IoT platform "Cloud of Things". The "Privacy and Security Assessment" method (PSA) provides for the integration of data security and data privacy in system and product development across the entire Group. The data centers have an early warning system for protection against cyber attacks. Extensive building protection safeguards the infrastructure against both unauthorized access and unexpected events such as fire, flooding or power failure.

A COMPREHENSIVE SECURITY PACKAGE PAVES THE WAY FOR COMPANY APPLICATIONS IN THE INTERNET OF THINGS

A special list of measures provides the Cloud of Things with additional protection.

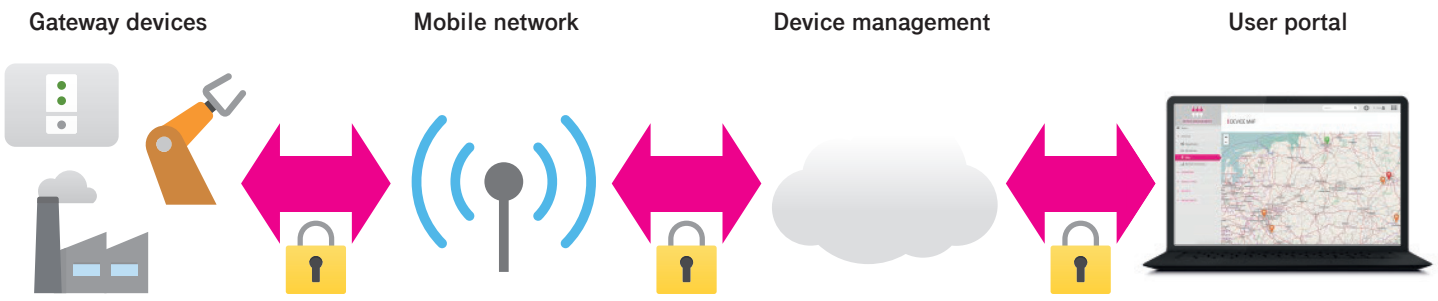
- The operating system and software are immunized against viruses and malware.
- All data is end-to-end encrypted (AES) and bidirectional TLS authentication precedes any network communication.
- Because databases and servers are actively managed, IT systems are protected against DDoS attacks.
- A multi-stage firewall provides protection against unauthorized access.
- Attacks on one Cloud of Things module cannot affect others because they all function independently from one another.
- Customer accounts are managed separately. No user can access another user's area.
- Customer data, user data and payload are stored independently, which ensures data privacy.

TLS AUTHENTICATION

The application of a recognized and standardized authentication mechanism ensures that no third parties can intervene in the communication with the Cloud of Things. The Transport Layer Security (TLS) protocol is used here. The communication partners check their authenticity by means of certificates and set up an encrypted connection. For security reasons, if a source is unable to provide sufficient proof of its identity, it is not trusted.

ENCRYPTION WITH AES

The "Advanced Encryption Standard" (AES) algorithm, authorized as a standard in the USA for top secret communications, is used to encrypt all data communication between the IoT devices and the platform, in both directions. For customers whose devices do not support AES, the Cloud of Things supports further encryption methods such as "3DES" or "Camellia".



CONTACT
- CloudderDinge@telekom.de
- +49 800 55 66 900
- iot.telekom.com

PUBLISHED BY
Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn, Germany

Status as of 01/2018 | Subject to error or change | X