Secure data protection in the new internet of things

8 July 2019

Credit: CC0 Public Domain

The core idea of the team headed by Magdeburg project leader, Professor Dr. Mesut Güne is to develop the self-organizing migration of services. This means that the services—such as home automation, data management, and business logic—no longer operate, as they have until now, centrally in a cloud, but instead can also act independently within a local infrastructure ecosystem. This local server infrastructure, which can also operate in small companies, or even on the computers of the user—or herself, guarantees full sovereignty over proprietary data. This allows companies to be independent of the server infrastructures of external service providers such as Google, Microsoft or Amazon, which are subject to constant changes and even may not be accessible.

"Smart devices can then operate with one another independently of the cloud and therefore work autonomously and fault-tolerantly," says Güne. "Due to the lack of need to share all data with the cloud, traffic and reaction time are reduced." This means the development of a technology that enables statutory regulations and industry standards on data security, reliability and privacy to be implemented in the Internet of Things.

According to Professor Güne, the background of the research project is the progressive digitalization of all areas of life due to changes in the way the Internet is used. "The Internet, as we know it, is based on network architectures from the 1970s and 1980s, when it was intended for entirely different applications." Previous systems of access control were either centralized, and thus became bottlenecks, or not flexible enough to cope with the dynamism of the access authorizations.

In order to bridge this gap, as part of the project, concepts are being developed that allow for transparent access to the data. Project partner, Professor Sebastian Zug is convinced that "For the application it should make no difference whether the specific information requirement is answered by a server or an IoT node."

"As a result, the systems benefit from one another, and can, for example, share computing capacities, data and so on," explains Mesut Güne. "A fast-growing data pool is being produced, which in turn makes it possible to produce considerably more accurate information, for example in the case of climate model forecasts, the observation of traffic flows or the management of large factories in Industry 4.0."

In this way, the opportunities and possibilities of the Internet of Things can be better exploited and simultaneously the possible risks be more manageable.

Provided by Otto-von-Guericke-Universität Magdeburg

APA citation: Secure data protection in the new internet of things (2019, July 8) retrieved 19 November 2019 from https://phys.org/news/2019-07-internet.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.