UBIRCH

THE NOTARY FOR SENSOR DATA

REGIO IT AND UBIRCH CREATE A FORGERY-PROOF LOGGING IN THE MICROSOFT AZURE CLOUD

In the Internet of Things, sensors collect tons of measurement data every day. The question of how companies store this data becomes crucial. An absolutely secure and traceable documentation of the measured values becomes indispensable in many areas - for safety and compliance reasons. The IT vendor in Aachen, regio iT, has developed a process together with the IoT specialists from UBIRCH in Cologne, with which sensor data can be „sealed", guaranteed to be immutable, and trusted to be stored in the Microsoft Azure Cloud. The use of blockchain technology guarantees the immutability of the data.

The challenge: keep sensitive sensor data tamper-proof

Many companies do not operate their own server centers, but use the servers of specialized providers such as regio iT. The terms of server usage are defined by customers and providers in a Service Level Agreement (SLA). So that the customer can check whether the operator complies

with the parameters of the operation of the server, he relies on sensor records. They record power supply, reaction times and temperature and save the values. Measurement data helps to detect whether parts need to be replaced or maintained and whether the IT system is running at the limit. In the event of discrepancies, the operator must provide the customer with proof of the correct control of the system. regio iT and the Microsoft partner ubirch rely on the Azure Cloud.

The solution: Blockchain and data storage in the Azure Cloud

Multiple components need to work together to keep the metrics from regio iT's data centers secure: the sensor, the storage solution in the Azure cloud, and the blockchain. First, a cryptographic method seals the data on the sensor. „This data notary confirms the authenticity of the data in a first step," says Markus Breuer from UBIRCH. Once collected, sealed, and encrypted, the solution transmits the data packets to the Azure Cloud, which receives and verifies them. To keep this data forgery-proof for the future, she first sums it up into „super packages" in a private blockchain and then stores their hash codes in a public blockchain. Because of these two steps, the data can be retrospectively checked: have they been changed? Is the order correct? Did the data have been duplicated? Which devices do they come from? „With UBIRCHs data notary, we can give a kind of quality and origin seal to data packages," explains Dieter Rehfeld from regio iT. The blockchain ensures that data manipulation is not possible.

However, the possible applications of this process are manifold for Dieter Rehfeld: „Smart cities, for example, already produce a great deal of traffic data. With the quality seal of the data notary, we can help to make data packets trustworthy and tradeable." The innovative solution from UBIRCH and regio iT guarantees the quality and integrity of the content of the packages for outsiders.

In cooperation with: Microsoft regio iT

Stephan Noller, CEO	Office Cologne	Office Berlin	Office Munich
stephan.noller@ubirch.com	Im Mediapark 5	Gürtelstr. 25	Ringseisstr. 3 Rgb
+49 171 972 77 50	50670 Cologne	10247 Berlin	80337 München
www.ubirch.com	Germany	Germany	Germany