Freenet as a broker for „Medical“ IoT Data

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Daniel Voisard

IoT devices are everywhere these days. However, all IoT devices have the same problem, if the manufacturer of the devices goes bankrupt, they no longer work. In this work we try to break this dependency, so that the device can be maintained independently and work even after the bankruptcy of a manufacturer.

Yannick Stebler
yannick@ystebler.ch

Introduction

IoT devices are on the rise and it is hard to imagine our everyday lives without them. They facilitate many everyday tasks, collect information or connect us with other people. New applications for these small and often practical devices are added every day. However, most of these IoT devices have a very big vulnerability. The data exchange of IoT devices is often handled by the manufacturer of the devices. This means that if a manufacturer goes bankrupt, that manufacturer's IoT devices become useless because the data exchange between the devices can no longer take place.

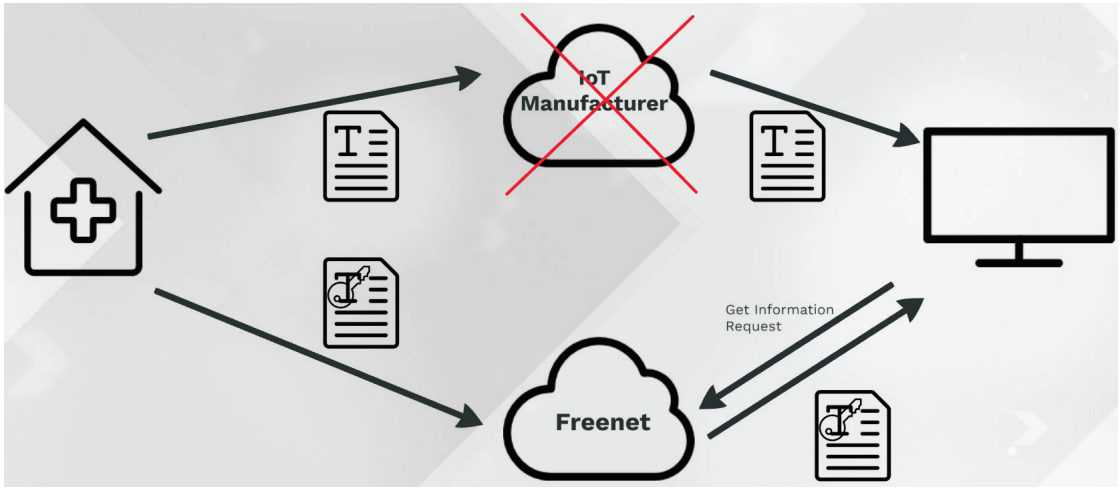
Breaking the dependency

Breaking this very issue of dependency between the IoT device and the manufacturer and allowing the devices to continue to be used via a newly defined communication path, even if the manufacturer goes bankrupt. Furthermore, when creating a new communication path, it is of high importance that all customer-relevant data is transferred anonymously and securely.

This new communication channel is created by means of a so-called broker (Freenet). This serves as an interface of communication (as a manufacturer replacement) between the IoT sender and the receiver. A new IoT transmitter is registered with the receivers using a QR code. After registration, a new node is negotiated between the sender and receiver over an insecure channel in Freenet. Subsequent communication via this node takes place over a secure channel. Patient-relevant data is now transmitted here in encrypted form.
After the sender has uploaded the data to Freenet, it is downloaded and verified by the receiver. If the data is correct and complete, an acknowledge message is sent to the sender via the same node so that the sender knows it can send the next data.

More to come

The potential of this work is immense, therefore there are several further works that can be developed. Other works that could be possible are the development of multidevice use. Performance improvements and scaling of the broker (decrease risk of flooding



Process overview