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 manufacturers can be maintained independently and work even after the bankruptcy of a manufacturer.

Introduction

IoT devices are on the rise and it is hard to imagine our everday life without them. They make many everday tasks easier, collect information or connect us with other people. New applications for these small and often practical devices are bein added everyday. However, the majority of these IoT devices have a very large weak point. The data exchange of the IoT devices is often handled by the manufacturer of the devices. This means that if a manufacturer goes bankrupt, the IoT devices from this manufacturer ofthen become useless, as the data exchange between the devices can no longer take place.

Goal

The goal of this work is to break the dependency between IoT device and manufacturer and to enable the devices to continue to be used via a newly defined communication path, even if the manufacturer goes bankrupt. Furthermore, all customer-relevant data is to be transmitted anonymously and securely.

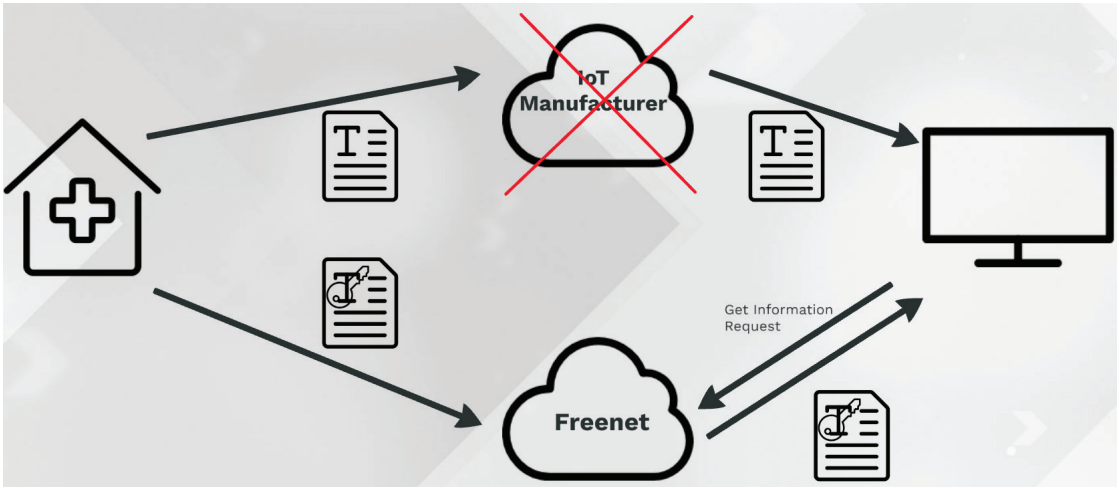
Implementation

A new communication path was implemented. The IoT devices now communicate with the recipients via a so-called broker (Freenet). A new IoT transmitter is registered on the receivers via a QR code. After registration, a new node is negotiated between the sender and receiver via an insecure channel on Freenet. Subsequent communication via this node takes place over a secure channel. Patient-relevant data is now transmitted here in encrypted form.
Once 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 that he can send the next data.

Future work

Future work would be to improve the performance of the communication, increase the scaling of the broker (reduce vulnerability to flooding). Creating libraries for use in different programming languages and for any kind of IoT devices.

Yannick Stebler
yannick@ystebler.ch



Process overview