DHBW
Duale Hochschule
Baden-Württemberg

IoT-Labor: Smart Lock

Dokumentation

Bachelor of Science

des Studiengangs Informatik

an der Dualen Hochschule Baden-Württemberg Stuttgart

von

Tom Freudenmann, Maximilian Nagel, Marcel Fleck

26.04.2023

Bearbeitungszeitraum	10.03. - 26.04.2023
Matrikelnummern, Kurs	6378195, 7362334, 9611872, INF20D
Dozent	Hartmut Seitter

Selbstständigkeitserklärung

Ich versichere hiermit, dass ich meine Dokumentation mit dem Thema: *IoT-Labor: Smart Lock* selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Stuttgart, 26.04.2023

Tom Freudenmann, Maximilian Nagel, Marcel Fleck

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

Inhaltsverzeichnis

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

Abkürzungsverzeichnis

BLE	Bluetooth Low Energy
GPS	Global Positioning System
HTTP	Hypertext Transfer Protokol
IoT	Internet of Things
JSON	JavaScript Objective Notation
LED	Light Emitting Diode
LoRa	Long Range (Low Power)
LoRaWAN	Long Range Wide Area Network
MQTT	Message Queuing Telemetry Transport
PIO	Programmed Input/Output
TTN	The Things Network

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

Abbildungsverzeichnis

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

1 Einleitung / Business Case

Im Rahmen des Internet of Things (IoT)-Labs widmeten sich die Studenten einem ganz bestimmten Problem: Vorhängeschlösser. Vorhängeschlösser kommen an vielen Orten zum Einsatz: zum Gartenhäuschen Verriegeln, in der Umkleide des Fitnessstudios, zum Fahrrad Abschließen, zum Garagentor Verriegeln und vielen anderen Einsatzgebieten. Diese Vorhängeschlösser bringen dabei allerdings ein ganz spezifisches Problem mit sich. Vorhängeschlösser werden mit einem Schlüssel ge- und entsperrt und haben damit ein hohes Verlustpotential. Die Schlüssel sind meist sehr klein und werden in einigen Fällen auch nicht häufig benötigt (Gartenhäuschen nur im Sommer).

Eine weitere Unannehmlichkeit ist beim Anwendungsfall des Fitnessstudios zu finden. Die Kabine wird meist lediglich mit einer Flasche für die Versorgung, einem Handtuch für die Übungsausführung und dem Handy zur musikalischen Begleitung oder anderem Entertainment während dem Training verlassen. Jetzt ist da aber noch der Spindschlüssel. Der passt irgendwie nicht ins Muster. In der Tasche, wenn die Sportbekleidung eine solche hat, ist der Schlüssel sehr unangenehm. Den Schlüssel in der Handyhülle zu verstauen ist meist nicht möglich, dafür ist der Schlüssel schlicht zu dick. Und da sonst keine Gegenstände mitgeführt werden, bietet sich keine vernünftige Verstauungsmöglichkeit für den Schlüssel an!

Hier kommt die IoT-Lösung Smart-Lock ins Spiel. Smart-Lock soll ein Vorhängeschloss sein, welches zuverlässig über eine Handy-App ver- und entriegelt werden kann. Dies behebt die Probleme des Schlüsselverlusts und der „Kruschtelei“ mit den kleinen Schlüsseln.

Wie die IoT-Lösung des intelligenten Schlosses umgesetzt wurde, was es für Funktionalitäten hat und wo eventuelle Hindernisse liegen, soll im Folgenden aufgeführt werden.

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

2 Architektur

Die entwickelte IoT-Lösung Smart Lock teilt sich in vier verschiedene Layer auf: Device-, Network-, Service- und Application-Layer. Abbildung 2.1 beschreibt den architektonischen Aufbau der Lösung genauer und enthält die verschiedenen Hardware und Software Module der Lösung.
Anhand dieser Abbildung beschreiben die folgenden Abschnitte, den architektonischen Aufbau der Komplettlösung. Hierbei wird auf die jeweiligen Architektur-Layer eingegangen und erklärt, welche Eigenschaften die abgebildeten Geräte, Protokolle und Software im Rahmen der IoT-Lösung mit sich bringen.

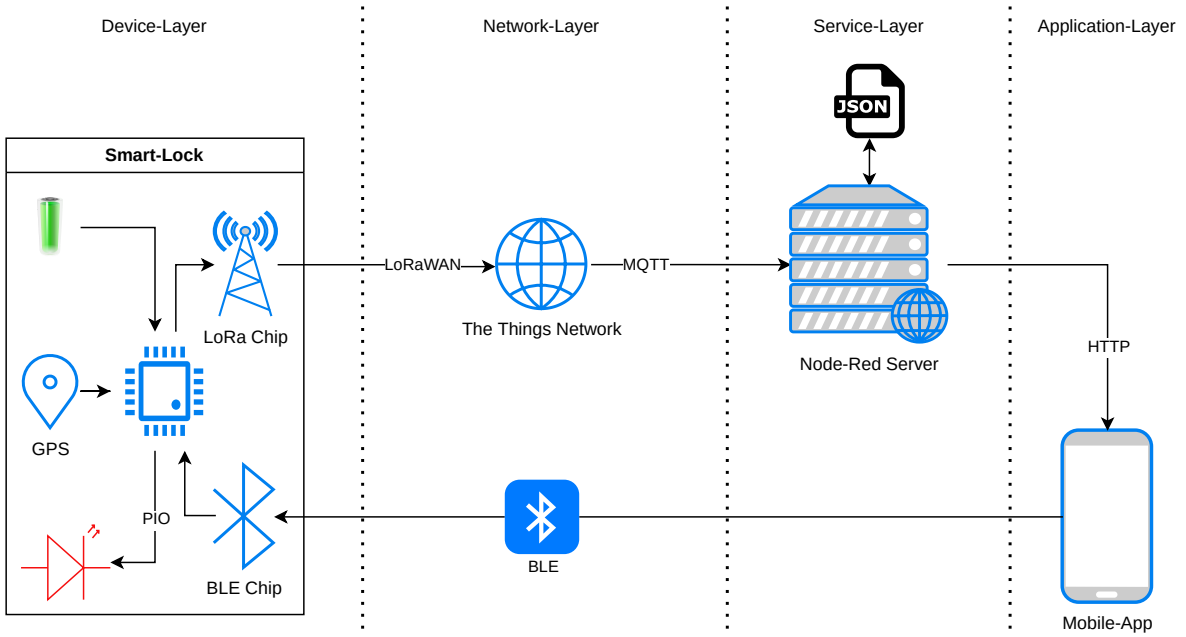


Abbildung 2.1: Architektur-Diagram des Smart-Locks

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

2.1 Device-Layer

Im Device-Layer finden sich alle Sensoren und Aktoren der IoT-Lösung wieder. Zu den Sensoren gehört ein Global Positioning System (GPS)-Chip, der GPS-Daten empfängt, um den Standort des Smart-Locks festzustellen.

GPS-Daten können in verschiedenen Darstellungsoptionen empfangen werden, darunter *GPGGA* und *GPRMC*. Da sich die empfangen Daten im Aufbau je nach Protokoll unterscheiden, muss eine Vorverarbeitung der Daten stattfinden, um genaue Positionsdaten zu erhalten. Hierfür werden die GPS-Daten, die in Form eines *Strings* empfangen werden, anhand der im Datenstring enthaltenen Kommatas getrennt. Um nun für Karten verwendbare Positionsdaten zu erhalten, müssen die ausgelesenen Positionsdaten in Grad und Minuten konvertiert werden. Nachdem diese Daten vorverarbeitet wurden sind diese Sendebereit.

Eine Light Emitting Diode (LED), die den Zustand des Smart-Locks, also ob geschlossen oder offen, darstellt, gehört zur Gruppe der Aktoren. Diese ist mit Hilfe eines Programmed Input/Output (PIO)-Pin direkt an den Mikrokontroller angeschlossen.

Des Weiteren befinden sich zwei Netzwerkschnittstellen in Form zwei gesonderter Chips im Device-Layer der IoT-Lösung. Ein Long Range (Low Power) (LoRa)-Chip dient dem Senden und dem Empfangen von LoRa-Nachrichten mit Hilfe von Long Range Wide Area Network (LoRaWAN) an das The Things Network (TTN). Ein Bluetooth Low Energy (BLE)-Chip ermöglicht eine Verbindung mit einem Mobilgerät und dient dem Empfangen von Befehlen, die den Zustand des Smart-Locks ändern können. Diese Netzwerkprotokolle werden in Kapitel 2.2 genauer beschrieben.

Die Stromversorgung ist durch einen eingebauten Akku auf der Platine des Mikrokontrollers sichergestellt.

2.2 Network-Layer

Das Network-Layer beschreibt die Protokolle und Netzwerk-Server, die die IoT-Lösung zum Austausch der Daten verwendetet. Dabei wird in der vorgestellten Lösung auf vier verschiedene übertragungstechnologien gesetzt.

Für die Übertragung der GPS-Daten wird **LoRaWAN** verwendet und sendet die Daten an ein Gateway. Das Gateway ist Teil des TTNs, ein zusammenschluss aus vielen

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

öffentlichen LoRaWAN-Gateways. Im TTN werden die Daten über einen Parser in ein JavaScript Objective Notation (JSON)-Format gebracht und können über herkömmliche Netzwerkprotokolle, wie Hypertext Transfer Protokol (HTTP)-WebSockets oder Message Queuing Telemetry Transport (MQTT) an einen Server übertragen werden.

Die vorgestellte Smart Lock Lösung verwendet für die weitere Übertragung an das Service-Layer **MQTT**. Das hat den Vorteil, dass sich Nachrichten sobald sie Empfangen werden, an den Server übertragen lassen und nicht über ein Request-Response verfahren abgefragt werden müssen.

Zusätzlich zu LoRaWAN und MQTT wird in der Lösung **HTTP** für die Kommunikation von App und Server verwendet. Hierfür sendet die Benutzer-App eine HTTP-Request an den Node-Red Server, der die Anfrage verarbeitet und die Device-Daten an die App zurücksendet.

Zuletzt wird **BLE** für das Öffnen und Schließen des Schlosses und somit für die direkte Kommunikation von App zu Device verwendet. BLE hat zwei entscheidende Vorteile: geringer Energieverbrauch und geringe Reichweite. Ersteres ist notwendig, damit das Schloss möglichst lange Akkulaufzeiten hat und zweiteres damit das Schloss nur aus unmittelbarer Nähe geöffnet oder geschlossen werden kann.

Zusammengefasst, deckt das Network-Layer die Kommunikation von allen verwendeten Hardware- und Software-Modulen ab und verwendet hierfür LoRaWAN über das TTN als Gateway zu MQTT, sowie HTTP und BLE für die Kommunikation zur Benutzer-App.

2.3 Service-Layer

Das Service-Layer besteht aus einem Node-Red Server, der in einem Docker-Container läuft. Das hat den Vorteil, das die Anwendung beliebig umgezogen oder skaliert werden kann. Zusätzlich empfängt der Server die Daten aus dem TTN über MQTT und speichert sie local in der *Context*-Variablen und persistent als JSON-Dokument ab. Dadurch können die Daten auch nach einem Neustart der Anwendung weiter verwendet werden. Abbildung 2.2 zeigt die folgenden drei Prozesse in Node-Red:

- **Initialisierung**: Der erste *Flow*, der beim Serverstart einmalig ausgeführt wird. Er lädt das gespeicherte JSON-Dokument und setzt die *Context*-Variablen auf die gespeicherten Werte.

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

- **Verbindung zum TTN-Server**: Dieser Prozess wird für jede im TTN empfangene und weitergeleitete Nachricht ausgeführt und speichert die empfangenen GPS- und Sensor-Informationen im JSON-Dokument bzw. Context des Servers.
- **App Anfrage**: Für jede empfangene HTTP-Anfrage an die Route *server-adresse:1880/device-id* wird der *Flow* ausgeführt. Er lädt die Daten für die mitgelieferte *device-id* und schickt sie als Antwort zurück and die App.

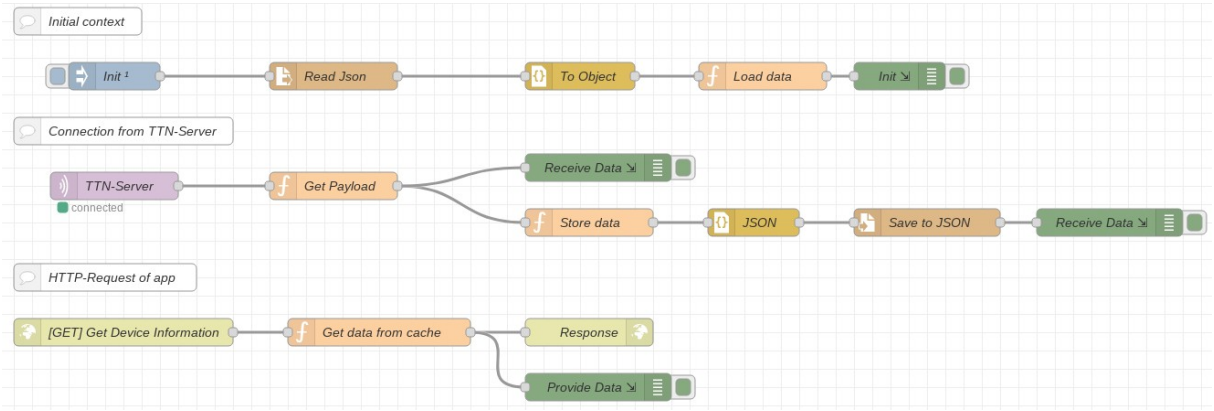


Abbildung 2.2: Node-Red Serverarchitektur für das Smart-Lock

Außerdem wird der Server in der Azure-Cloud, auf einem Ubuntu-Server gehostet. Dadurch ist der Server aus dem Internet zugänglich und die Daten können jeder Zeit vom Benutzer abgerufen werden.

Zusammengefasst, deckt der Server das Service-Layer mit persistenter Speicherung ab, indem er Nachrichten aus dem Network-Layer empfängt und an das Application-Layer weiterleitet. Zusätzlich werden die Daten im Server gespeichert, um sie jeder Zeit abfragen zu können, auch wenn der Server neu gestartet wurde. In Zukunft lässt sich das System weiter skalieren oder auf einem eigenen Server hosten, da es in einem Docker-Container läuft.

2.4 Application-Layer

Die vierte Schicht des IoT-Application Stack ist das Application Layer. Im Application Layer geht es darum, die vernetzten Geräte für den Nutzer verwendbar zu machen. Hierfür werden Applikationen entwickelt. Im Falle des IoT Smart-Locks sollte dies eine Handy-Applikation sein, welche die Kommunikation des Nutzers mit dem Schloss ermöglicht.

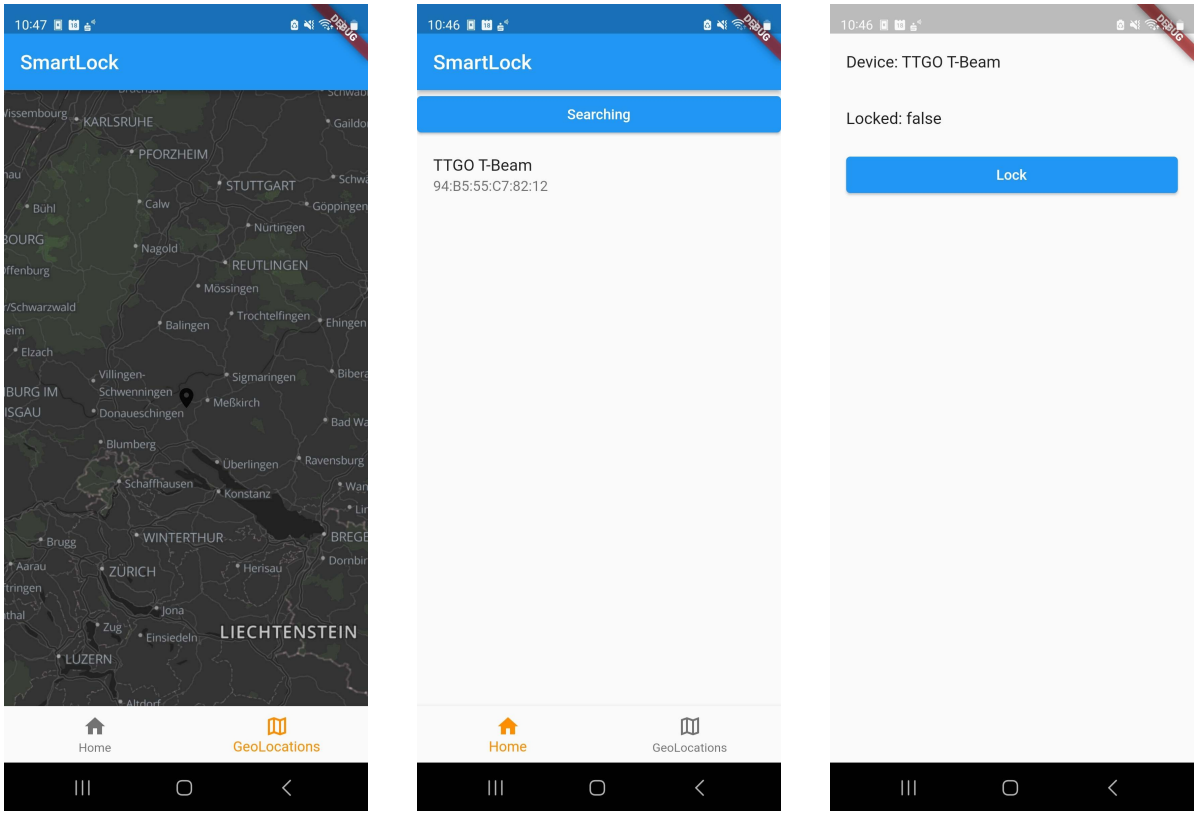
Die Anforderungen an die App sind recht simpel: Der Nutzer soll die Schlösser in der App angezeigt bekommen und nahegelegene Schlösser entsperren können. Die Anzeige soll

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

zweiermaßen ermöglicht werden. Einerseits soll eine simple Liste die Schlösser aufführen. Zusätzlich soll auch eine Karte die Geo-Positionen der Schlösser mit hoher Genauigkeit anzeigen, um speziell dem Verlustpotential entgegenzuwirken. Der Nutzer soll nahegelegene Schlösser entsperren können. Der Zusatz nahegelegen ist hierbei wichtig, da die Ver- bzw. Entriegelung des Schlosses aus großer Distanz möglich sein soll.

Die App setzt genau obige Anforderungen um. Mithilfe einer Navigation Bar kann zwischen der Listen- und der Kartenansicht gewechselt werden. Nahegelegene Schlösser können Ver- und Entriegelt werden. Dem Benutzer werden alle Schlösser sowohl in der Such-Liste, als auch auf der Karte angezeigt (Abbildung 2.3b, 2.3a).

Die Kommunikation der App läuft zweigeteilt: Zum einen empfängt die App die Geo-Positionen der Schlösser über HTTP von dem Node-Red Server. Zum anderen kann über die BLE-Konnektivität des Smartphones mit nahegelegenen Schlössern kommuniziert werden (Abbildung 2.3c).



(a) Karte mit markierter Position (b) Suche nach Schloss über BLE (c) Verbundenes Schloss Öffnen und Schließen

Abbildung 2.3: Smart Lock App: Aufbau

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.

3 Ausblick

1. Sicherheit: Übertragung und Verbindung zu Schloss
2. Updates?!
3. Real umsetzen: Pricing
4. Langfristig Datenbankunmgebung
5. Abschluss: Gute initiale Grundlage für weitere Entwicklung

Duale Hochschule Baden-Württemberg Stuttgart – Studiengang Informatik, Tom Freudenmann, Maximilian Nagel und Marcel Fleck © Alle Rechte bei Tom Freudenmann, Maximilian Nagel und Marcel Fleck, auch für den Fall von Schutzrechtsanmeldungen. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht bei uns.