Standort-basierte Daten via MQTT

Seminararbeit “Webservice Security”

Marco Wettstein

2015-05-14

Contents

1 Einleitung

2 Ausgangslage

2.1 Timetraces

Im Rahmen einer Seminararbeit wurde für die Controlling- und Zeiterfassungs-Applikation "controllr" (siehe Abbildung 1) eine neue Client-Anwendung gebaut, welche durch die Integration verschiedener Dienste wie Github, Redmine und Google Calendar eine Art Protokoll der geleisteten Arbeit erstellt. Aus den Einträgen dieses Protokoll können in der Anwendung direkt Zeiteinträge in "controllr" erstellt werden. Abbildungen 2 zeigt das Arbeitsprotokoll von *TimeTraces*. Durch Anwählen eines Eintrages wird eine vor-ausgefüllte Eingabemaske angezeigt, welche den Zeiteintrag über eine REST-Schnittstelle an "controllr" sendet (Abbildung 3).

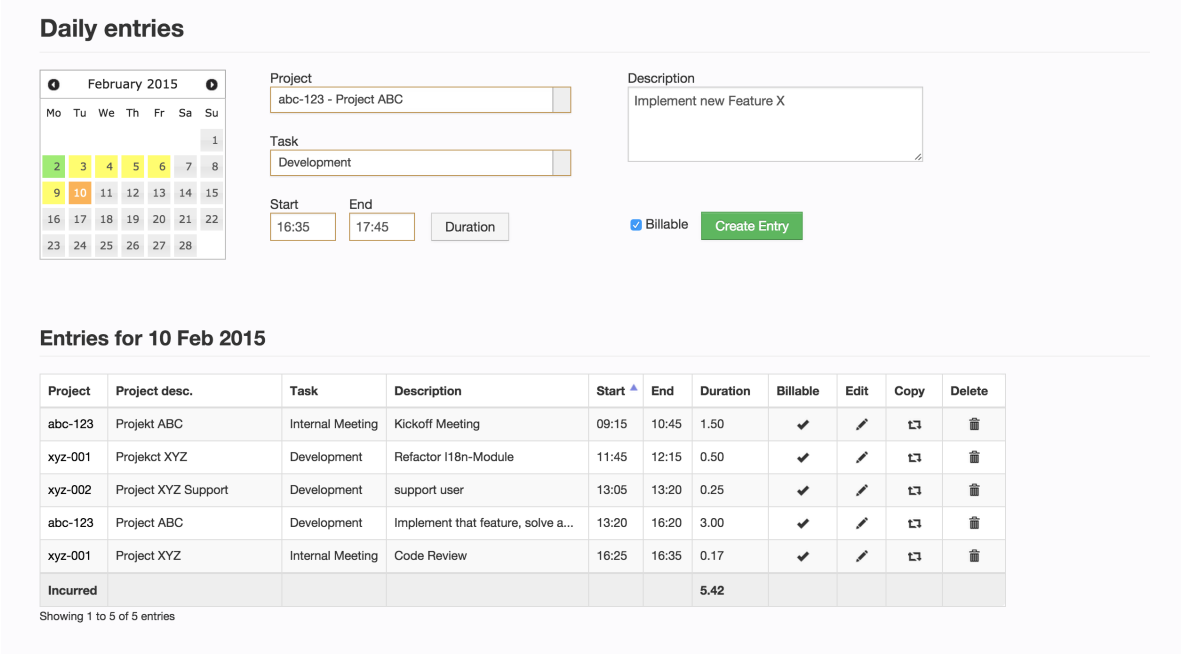

Figure 1: Screenshot von "Controllr" (Quelle (Wettstein, 6))

TimeTraces wurde als "Meteor"-Anwendung gebaut (siehe dazu Abschnitt **??**) und ist eine Client-Server-Anwendung, welche externe Dienste integriert. Die Anwendung speichert dabei ausser den Benutzer-Logins und den Einstellungen der Benutzer keine weiteren Daten (Siehe Abschnitt 2.1.2). Sämtliche Daten werden dabei vom Serverteil der Anwendung aggregiert und an den Client gesendet. Die Daten werden vom Server dabei über REST-Schnittstellen in einem Polling-Verfahren abgerufen. Das Polling wird gestartet, sobald der clientseitige Teil der Anwendung die Daten über eine DDP-Subscription abonniert und beendet, sobald der Client die Subscription beendet.

Abbildung 4 zeigt den Ablauf einer Subscription eines Clients.

2.1.1 Standortverlauf als weitere Event-Quelle

TimeTraces nutzt bisher *Github*, *Google Calendar* und *Redmine* als Event-Quellen. Als weitere Event-Quelle soll nun der Standort-Verlauf des Benutzers genutzt werden. Diese Daten sollen dem Benutzer helfen, die Zeiteinträge genauer zu erfassen. Der Benutzer sieht somit nicht nur, was wann gearbeitet

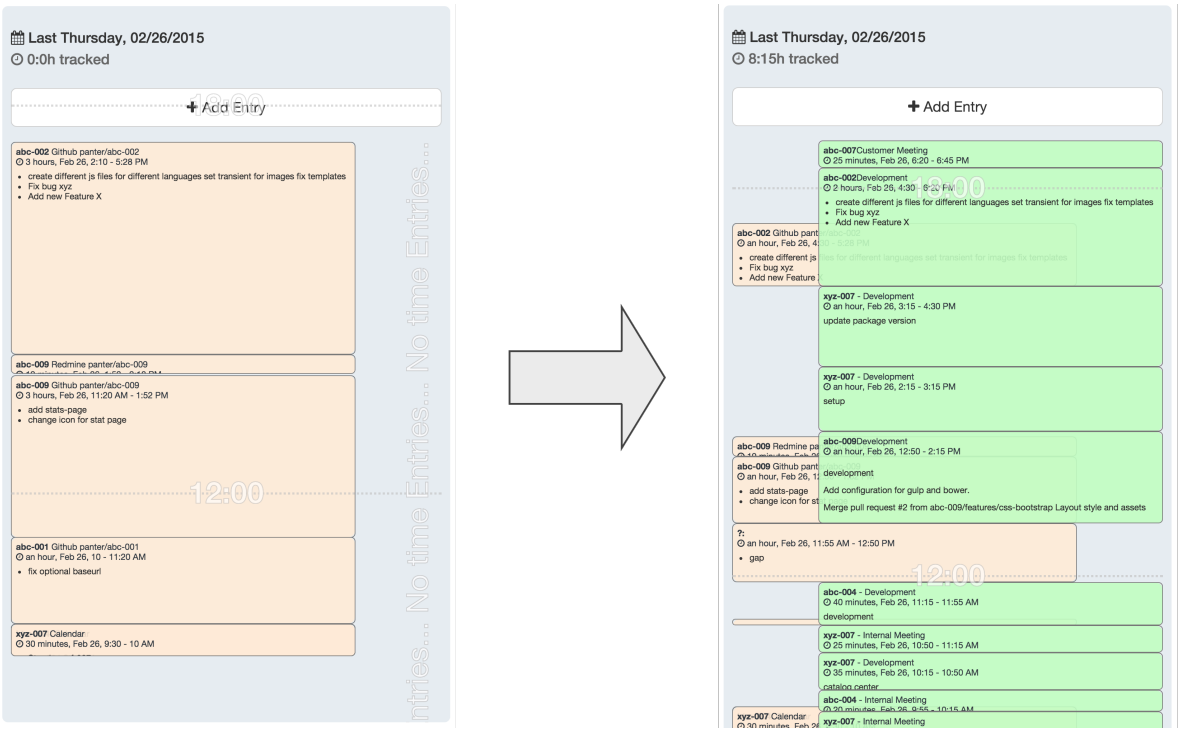

Figure 2: Darstellung der Event-Liste eines Tages in *TimeTraces*. Quelle (Wettstein, 22)

wurde, sondern auch wo. Es löst zudem das Problem, dass es oft schwierig ist, sich an den Startzeitpunkt einer Arbeit zu erfassen: es kann z.b. festgestellt werden, wann das Büro betreten wurde.

2.1.2 No-Data-Konzept

Im Zeitalter von Cloud-Computing ist es schwierig geworden, genau zu bestimmen, wo die Daten eines Benutzers überall sind und wer die Kontroller über diese Daten hat.

Beim Design von *TimeTraces* wurde dies berücksichtig, indem nur die nötigsten Daten, wie Einstellungen von Benutzer gespeichert werden. Die verwendeten Daten der Event-Quellen, wie Kalender udn Github werden dabei nicht dupliziert und gespeichert, sondern lediglich an die Client-Anwendung weitergeleitet.

2.2 OwnTracks

Owntracks wurde als Ersatz für den eingestellten Google Standort-Dienst “Latitude” entwickelt und ursprünglich in Anlehnung an das Vorbild und dem Verwendeten Protokoll als *MQTTitude* bezeichnet.[1]

Die Anwendung zeichnet den Standort des Benutzers im Hintergrund auf und sendet die Daten an einen zu definierenden MQTT-Broker unter einem wählbaren *Topic* (Siehe Abschnitt 5.2.5). Dabei können verschiedene Einstellungen wie die Häufigkeit der Standortprotokollierung

OwnTracks ist als quelloffene Anwendung für IOS und Android erhältlich und ist unter der *Eclipse Public Licence* veröffentlicht.[2]

[1] Siehe Quelle (“OwnTracks”)
[2] Lizenz und Quelle unter (“OwnTracks Lizenz”)

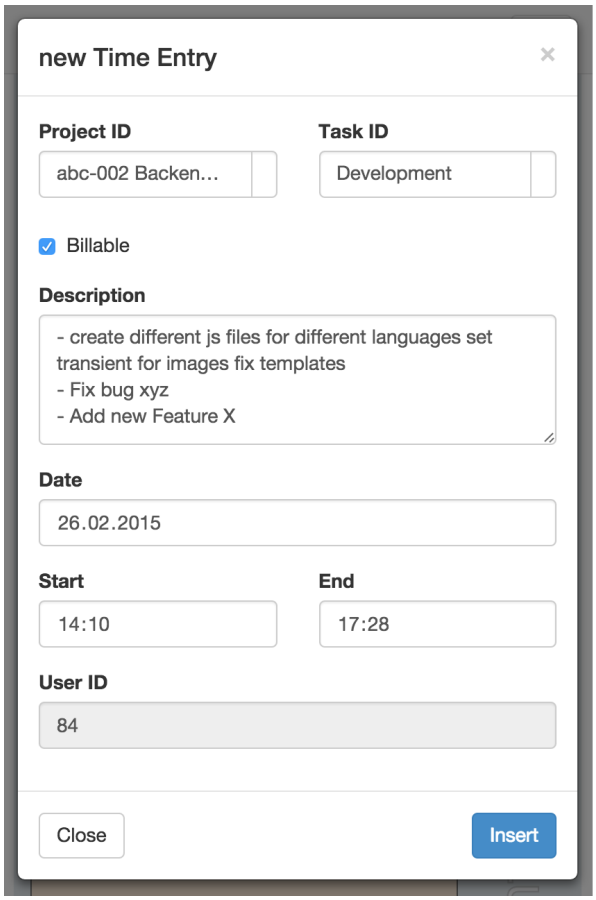

Figure 3: Eingabemaske für einen Zeiteintrag in *TimeTraces*. Alle Felder werden vorausgefüllt. Quelle (Wettstein, 23)

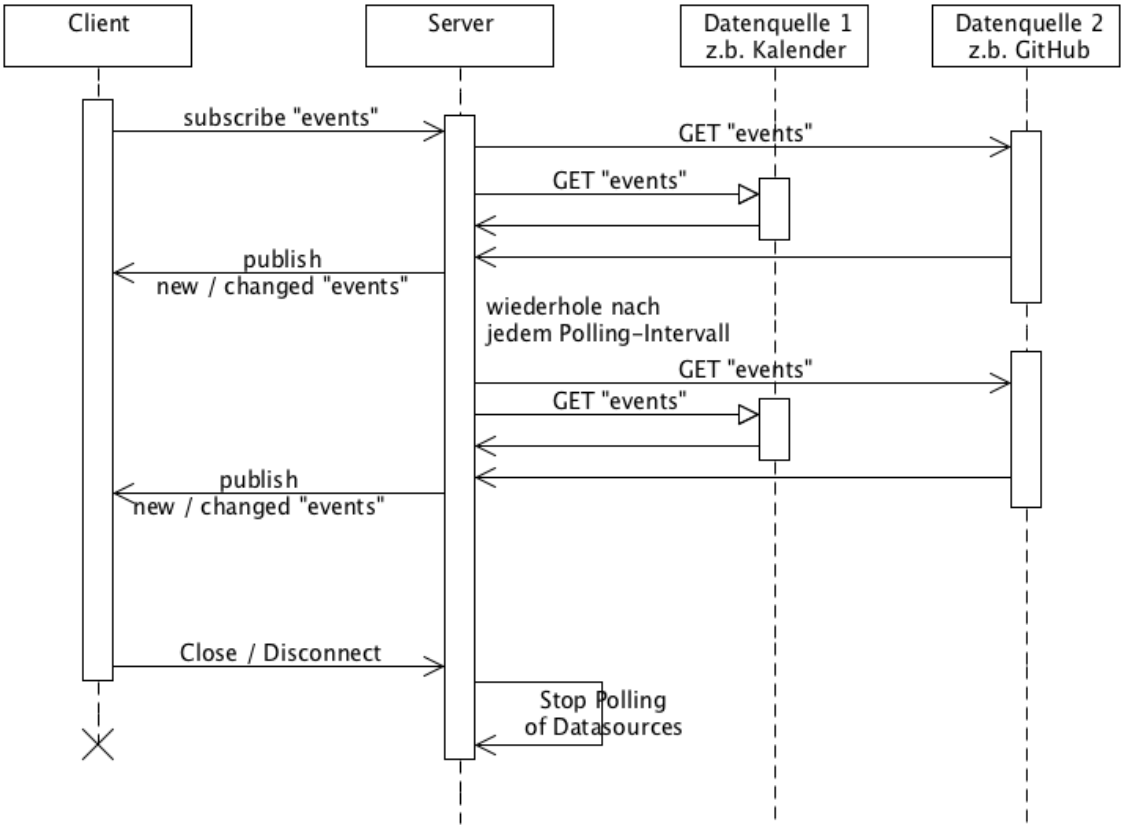

Figure 4: Ablauf einer Subscription von *TimeTraces* zwischen Client - Server und externen Quellen. Quelle (Wettstein, 19)

Die Verwendung von *OwnTracks* ist im Rahmen dieser Arbeit als Ausgangslage vordefiniert und gibt das Protokoll *MQTT* vor, es sollen aber auch Alternativen betrachtet werden[3]

[3]Owntracks nutzt MQTT als Übertragungsprotokoll. Es ist aber auch denkbar, dass anderen Anwendungen ein anderes Protokoll verwenden.

3 Zielsetzung

Die Ziele dieser Arbeit sind

- Vertiefung in das Thema MQTT
- Betrachtung sicherheitsrelevanter Aspekte von MQTT,
- Betrachtung generell sensitiver User-Daten, wie Standortverlauf
- Setup einer geeigneten MQTT-Broker-Lösung mit geeigneten Sicherheitseinstellungen
- Verbinden von "OwnTracks" oder einer ähnlichen Anwendung und *TimeTraces* via MQTT und dem gewählten Broker

4 Konzept

Auf einem mobilen Endgerät des Benutzers soll eine Anwendung laufen, welcher seinen Standort periodisch an eine zentrale Stelle übermittelt.

Die Anwendung *TimeTraces* wird um eine Funktion erweitert, welche diese Daten abfragt und auswertet. Der Benutzer soll dabei sehen, zu welchem Zeitpunkt er sich an welchem Standort aufgehalten hat. Die Daten werden also nicht in Echtzeit benötigt (wie es beispielsweise häufig bei Standort-basierter Werbung der Fall ist), sondern mit Verzögerung (einige Tage bis wenige Wochen).

Es ist daher nötig, die Daten Zwischenzuspeichern um sie später auszuwerten.

5 Recherche

5.1 Location-Apps & -Dienste

https://play.google.com/store/apps/details?id=com.glympse.android.glympse http://onetouchlocation.creativeworkline.com

5.1.1 Owntracks

tODO: runter schieben?

5.1.2 Google+

TODO

5.2 MQTT

MQ Telemetry Transport oder kurz *MQTT* ist ein Protokoll für die Maschine-zu-Maschine-Kommunikation von Telemetrie-Daten. MQTT wurde insbesondere für Leistungsschwache Endgeräte entwickelt, sowie für Netzwerke mit hoher Verzögerung oder geringer Leistung. So wurde MQTT auch für die Kommunikation über Satelliten genutzt.[4]

MQTT wurde 1999 von Dr Andy Stanford-Clark (IBM) und Arlen Nipper (Arcom, Eurotech) entwickelt.[5]

5.2.1 Netzwerklayer und Sicherheit

MQTT ist im TCP/IP-Referenzmodell in der Anwendungs-Schicht angesiedelt und nutzt TCP als Übetrtragungsprotokoll. Die Übetragung kann mittels SSL/TSL verschlüsselt werden, allerdings erhöht das den Leistungsbedarf der Übertragung signifikant. MQTT sieht innerhalb des Protokolles keine Verschlüsselung vor, es ist jedoch möglich, sich mittels Benutzername und Passwort zu authentifizieren.[6]

Mit *MQTT-SN* steht eine Variante für nicht-TCP/IP-Netzwerke, wie *ZigBee* zur Verfügung.[7]

[4] Siehe Einleitung unter der Offiziellen Seite von MQTT (**???**).
[5] Siehe ("MQTT - Frequently Asked Questions")
[6] Siehe ("MQTT - Frequently Asked Questions")
[7] Siehe ("MQTT for Sensor Networks – MQTT-SN").

5.2.2 Anwendungen

Durch diese Optimierungen ist MQTT für Sensoren, wie Temperatur-, Feuchtigkeits oder Durckmesser, Lichtschalter, Bewegungsmelder und Aktoren, wie Lampen, Motoren, Relais oder ähnliches geeignet. MQTT wurde 2013 als Protokoll des *Internets der Dinge* standardisiert und bietet somit beispielsweise eine standardisierte Übertragungsmöglichkeit für die Hausautomation.[8]

Durch die geringe Leistungsaufnahme ist MQTT ebenfalls geeignet für mobile Endgeräte, wie Smartphones, wo lange Akkulaufzeit und geringe Datenübertragung wünschenswert sind.

5.2.3 Topics und Publish-Subscribe

MQTT folgt dem Konzept einer *Message oriented Middleware* und ermöglicht das *Beobachter-Entwursfmuster*, welches auch *publish-subscribe* genannt wird.[9] Dabei *abonnniert* ("subscribe") ein Client ein bestimmtes *Topic*. Ein Client kann auf ein *Topic* eine Nachricht *veröffentlichen* ("publish"), welche dann alle Clients erhalten, die dieses *Topic* abbonniert haben. Ein *Broker* dient dabei als Vermittler zwischen den Clients und leitet die Nachrichten an die für sie bestimmten Clients weiter. (Siehe Abschnitt 5.2.5)

5.2.4 Qualitiy of Serivce (QoS)

MQTT sieht 3 Stufen für die Übertragungs-Qualität einer Nachricht vor:

QoS 0 - At most once delivery: Die Nachricht wird **höchstens einmal** zugestellt. Nachrichten mit QoS 0 können verloren gehen, wenn ein Client die Verbindung unterbricht oder ein Broker offline ist. Der Vorteil an QoS 0 liegt primär in der Performance, da Nachrichten nicht zwischengespeichert und nicht protokolliert werden muss, welcher Benutzer welche Nachricht erhalten hat.

QoS 1 - At least once delivery: Clients und Broker versuchen, die Nachrichten **mindestens einmal** zuzustellen. Es ist möglich, dass Nachrichten mehrfach zugestellt werden.[10]

QoS 2 - Exactly once delivery: Diese Stufe garantiert, dass eine Nachricht genau einmal zugestellt wird. Die Stufe stellt somit wie QoS 1 den Empfang einer Nachricht sicher und vermeidet dabei Duplikate. QoS 2 stellt somit die höchste Qualitätsstufe der Übertragung dar und erfordert damit auch mehr Komplexität und Rechenleistung in Client und Broker.

5.2.5 Broker

Broker verbinden die verschiedenen Clients und dienen als Vermittler der Nachrichten. Sie nehmen Nachrichten von Clients entgegen und senden sie an andere Clients, welche das *Topic* der Nachricht abbonniert haben. Broker berücksichtigen dabei die QoS-Stufe der Nachricht und müssen bei entsprechender QoS-Stufe Nachrichten auch Zwischenspeichern.

[8] Quelle ("Wikipedia - MQ Telemetry Transport")
[9] Siehe Quelle [ˆfn_observer_pattern].
[10] Die in der Quelle ("What Is MQTT and How Does It Work with WebSphere MQ?") angebene Seite zeigt eine Übersicht über MQTT und die Verschiedenen QoS-Level.

5.3 Verfügbare MQTT-Broker

5.3.1 Mosquitto

Mosquitto ist ein quelloffener MQTT-Broker und wurde unter der BSD-Lizenz veröffentlicht. Für verschiedene Plattformen und Betriebsysteme stehen vorkompilierte Pakete als Download oder in Paketmanagern zur Verfügung.[11]

Der Broker kann auf einem eigenen Server installiert werden, setzt somit aber bestehende Infrastruktur voraus.

Mosquitto speichert Daten im Arbeitspeicher und persistiert die Daten periodisch auf den Datenträger. [ˆfn_mosquitto_ autosave_interval]

Weiterhin kann Mosquitto sich mit weiteren Brokern via *Bridge* verbinden.[12]

[ˆfn_mosquitto_ autosave_interval]: Siehe Option * autosave_interval* in Quelle (“Mosquitto General Options”)

5.3.1.1 Verschlüsselung und Authentifizierung

Mosquitto erlaubt Zertifikat-basierte Veschlüsselung mittels TLS/SSL. Der Server weisst dabei an den Client ein Zertifikat aus, welches der Client verifiziert. Umgekehrt besteht die Option, dass der Client sich gegenüber dem Server ebenfalls mit einem Zertifikat authentifizieren muss. Dies kann dazu genutzt werden, einen User zu identifzieren. Ohne Client-Zertifikat ist auch eine Authentifizierung mittels Benutzername und Passwort möglich. Statt eines Zertifikates kann auch ein *pre-shared-key*-Verfahren genutzt werden, wobei vorgängig ein Schlüssel ausgetauscht wird.[13]

Nutzt mann die Client-Authentifizierung, so ist es möglich, die Zugriffsrechte eines Clients auf einzelne Topics einzuschränken. Dabei können für ein Topic reine Lese- und Schreibrechte oder Beides vergeben werden.[14] Es ist darüber hinaus auch möglich, nicht-authentifizierte Benutzer auszuschliessen.

Mosquitto unterstützt weiterhin die Kommunikation über Websockets, d.h. es kann via Websockets direkt mit dem MQTT-Broker kommuniziert werden.

5.3.2 HiveMQ

HiveMQ ist ein laut Hersteller für Unternehmen optimierter MQTT-Broker und zeichne sich durch hohe Performance, gute Skalierbarkeit (durch Clustering), hohe Sicherheit, sowie 100%iger MQTT 3.1.1 Unterstützung überzeugen.

Wie Mosquitto untertützt HiveMQ Kommunikation über Websockets, (X509) Zertifikat-Authentifizierung, sowie Bridging.

HiveMQ ist kostenpflichtig, es stehen monatliche Lizenzen oder einmalige Lizenzen zur Verfügung. Die Kosten für die einmalige Lizenz bewegen sich zwischen 325 € und 6250 €. Eine kostenlose Testversion steht ebenfalls zur Verfügung.

[11] Siehe (“Mosquitto Homepage”)
[12] Siehe (“Mosquitto Bridges Options”)
[13] Siehe (“Mosquitto Authenfication”)
[14] Siehe Option * acl_file* in Quelle (“Mosquitto General Options”)

5.3.3 Moquette

Moquette ist ein Quelloffener MQTT-Broker, welcher in Java implementiert ist. Er steht unter der Apache License 2.0.

Der Broker wird aktiv weiterentwickelt, unterstützt aber weniger Funktionen von MQTT als Mosquitto oder HiveMQ. So ist es u.a. noch nicht möglich, Zugriffsrechte für einzelne User zu setzen. QoS 0,1 und 2 werden unterstützt.[15]

5.3.4 Mosca

Dieser Broker ist als *node.js*-Applikation und über den *Node Package Manager* (*npm*) erhältlich. Er kann direkt als Broker genutzt werden oder in einer anderen *node.js*-Applikation als Modul genutzt werden.

Mosca ist MQTT 3.1 kompatibel, unterstützt aber nur QoS 0 und 1. Nachrichten können auf einer MongoDB oder Redis-Datenbank persistiert werden.

Der Quellcode von Mosca ist unter Github veröffentlicht, es ist allerdings keine Lizenz angegeben.[16]

5.3.5 GnatMQ

GnatMQ ist ein auf dem .NET-Framework von Microsoft basierender MQTT-Broker. Er unterstützt alle 3 QoS-Stufen, Authentifizierung via Benutzername/Passwort, sowie Zugriffskontrolle, jedoch noch keine SSL/TLS-Verbindunng und kein *Bridge*-Modus.

5.3.6 Gehostete MQTT-Broker

Statt einer selbst verwalteten Lösung, kommen auch Cloud-Dienste in Frage (*software as a service*).

5.3.6.1 CloudMQTT *CloudMQTT* ist ein gehosteter MQTT-Broker. Es gibt ein kostenloses Abonnement und zwei kostenpflichtige ($19, resp. $99 pro Monat).

Der Dienst unterstützt u.a. Authentifizierung, Zugriffskontrolle (*ACL*), *Bridge*-Modus, sowie Kommunikation über Websockets.

[17]

5.3.7 Vergleich

5.3.7.1 Self-Hosted gegen Cloud-Lösung Bei Standort-Daten handelt es sich um sensible Daten. Diese besitzen auch einen gewissen *Business Value*, was bei Standort-basierter Werbung zu sehen ist. Bei Cloud-Lösungen wird die Kontrolle über diese Daten an einen Fremdanbieter abgegeben. Im Rahmen dieser Arbeit ist dies zweitrangig; in einer produktiven Anwendung ist dies aber nicht zu vernachlässigen.

Cloud-Lösungen bieten aber den Vorteil des einfacheren Setup. Skalierung und Betrieb kann ebenfalls an den Anbieter abgegeben werden.

[15] Siehe (“Github Moquette”)
[16] Siehe (“Github Mosca”)
[17] (“CloudMQTT”)

5.3.7.2 Detailvergleich (TODO: Tabelle)

5.3.8 Wahl

Alle untersuchten Broker kämen prinzipiell in Frage (bei den Kostenpflichtigen in einer Test-Version), die Wahl fiel jedoch auf Mosquitto, da dieser sehr gut dokumentiert ist und sehr viele MQTT-Features unterstützt. Somit kann sich mit vielen Aspekten von MQTT auseinandergesetzt werden.

Für die Installation steht u.a. eine (virtuelle) Ubuntu Instanz (12.04 LTS) in einem Rechenzentrum zur Verfügung.

6 Design

6.1 Sicherheitsapsekte

6.1.1 Sensible Daten

Standortdaten sind sicherheitsrelevant. Es handelt sich um sensible Daten, die insbesondere vor Missbrauch geschützt werden müssen.

6.1.2 Verschlüsselung

TODO

6.1.3 Authentifizierung

TODO

6.2 Architektur

Wie in Abschnitt 4 erwähnt, werden die Daten nicht in Echtzeit, sondern mit Verzögerung benötigt. Es ist also nötig, die Daten zwischenzuspeichern.

Da die Anwendung *TimeTraces* ein Server-Teil hat, könnte dieser für die Standortdatenspeicherung in Frage kommen.

Dagegen spricht aber, dass *TimeTraces* aus konzeptuellen Überlegungen keine Event-Daten speichert (siehe Abschnitt 2.1.2). Möchte man dieses Konzept beibehalten, so muss das Speichern der Daten auf eine andere Anwendung verlagert werden.

Die Broker-Software *Mosquitto* selbst kommt dafür ebenfalls nicht in Frage, da MQTT mit QoS 1 und 2 zwar Nachrichten persistiert, für eine ein- oder mehrwöchige Zwischenspeicherung ist ein Broker aber nicht ausgelegt.

6.3 Standort-Service als Brücke

Um dieses Problem zu lösen, kann ein Service erstellt werden, der zwischen *TimeTraces* und dem MQTT-Broker *Mosquitto* vermittelt. Da *TimeTraces* auf *Meteor* basiert, bietet es sich an, diesen Brücken-Dienst ebenfalls als Meteor-Applikation zu erstellen und zu *TimeTraces* via *DDP* zu kommunizieren.[18] Prinzipiell können die Standort-Daten auch über eine REST-Schnittstelle an *TimeTraces* übermittelt werden, da sie nur in eine Richtung gesendet werden. Da es sich aber bei *MQTT* und *DDP* Message-Oriented-Middleware handelt mit dem Publish-Subscribe-Muster, bietet es sich an, *DDP* für die Übertragung zu verwenden.

[18] Eine Evaluation möglicher Technologien für einen solchen Service ist nicht Teil dieser Arbeit. Die Wahl der Technologie basiert hier auf Vorwissen und Erfahrung des Autors.

6.4 Konzeption eines Standort-Services

6.4.1 Rollen

Der Standortservice benötigt zwei Rollen: der *Benutzer*, welche den Dienst nutzt und den *Administrator*, welcher den Dienst betreut und betreibt.

Weiterhin findet eine *Mashine-to-mashine*-Kommunikation mit dem vorgelagerten MQTT-Broker und der nachgelagerten Anwendung *TimeTraces* statt.

6.4.2 User-Stories

(TODO): Story-Cards

- Als Benutzer möchte ich mich für den Service registrieren können
- Als Benutzer möchte ich mich an den Service anmelden können
- Als Benutzer möchte ich meine Standort-Protokoll-Anwendung (z.b. *Owntracks*) mit dem Dienst verbinden können
- Als Benutzer möchte ich meine Standortdaten über eine Schnittstelle abfragen können
- Als Benutzer möchte ich Standort-Einträge löschen können.

6.4.3 System

6.4.4 Sicherheitsaspekte

Der Dienst kommuniziert mit zwei weiteren Diensten und benötigt daher auch zwei Übertragungskanäle, welche potentielle Sicherheitsrisiken bergen.

Beide Kanäle müssen über eine aktuelle Technologie verschlüsselt werden.

6.4.4.1 Datenschutz Der Dienst speichert die schützenswerten Standort-Daten und muss entsprechend vor Missbrauch geschützt werden.

(TODO NFR):

- Ein angemeldeten Benutzer kann nur seine Standort-Daten auslesen und bearbeiten
- Ein nicht-angemeldeter Benutzer kann keine Daten sehen
- Die Zugriffsdaten für einen Benutzer müssen hinreichend geschützt sein.

7 Umsetzung

TODO

7.1 Screenshots

TODO

8 Diskussion

TODO

9 Ausblick

9.1 Indoor-Standorte mittels Beacons

Generischer Event-Service

"CloudMQTT." http://www.cloudmqtt.com/.

"Github Moquette." https://github.com/andsel/moquette.

"Github Mosca." http://mcollina.github.io/mosca/.

"Mosquitto Authenfication." http://mosquitto.org/man/mosquitto-conf-5.html#idp49111296.

"Mosquitto Bridges Options." http://mosquitto.org/man/mosquitto-conf-5.html#idp49322480.

"Mosquitto General Options." http://mosquitto.org/man/mosquitto-conf-5.html#idp49117824.

"Mosquitto Homepage." http://mosquitto.org/.

"MQTT - Frequently Asked Questions." http://mqtt.org/faq.

"MQTT for Sensor Networks – MQTT-SN." http://mqtt.org/tag/mqtt-s.

"OwnTracks." https://github.com/owntracks/owntracks/wiki.

"OwnTracks Lizenz." https://github.com/owntracks/android/blob/master/LICENSE.

Wettstein, Marco. "TimeTraces - Seminararbeit 'Entwickeln von Anwendungen Für Hand Held'."

"What Is MQTT and How Does It Work with WebSphere MQ?" https://www.ibm.com/developerworks/mydeveloperworks/blogs/aimsupport/entry/what_is_mqtt_and_how_does_it_work_with_websphere_mq?lang=en.

"Wikipedia - MQ Telemetry Transport." http://de.wikipedia.org/wiki/MQ_Telemetry_Transport.

. http://mqtt.org/.