IoT Järjestelmän Toteutus

Harjoitussuunnitelma

Antti Kettunen

Hannu Oksman

Pekka Sivusuo

Antti Tarvainen

Saku Tupala

Harjoitustyö

11.2018

Tieto- ja viestintätekniikan koulutusohjelma

Tekniikan ja liikenteen ala

Sisällys

[1 Johdanto 2](#_Toc531887604)

[2 Teoria 2](#_Toc531887605)

[2.1 Bluetooth 2](#_Toc531887606)

[2.2 MQTT 2](#_Toc531887607)

[2.3 JSON 2](#_Toc531887608)

[2.4 RuuviTag 2](#_Toc531887609)

[2.5 Ubuntu Server 18.04 3](#_Toc531887610)

[3 Suunnitelma 3](#_Toc531887611)

[4 Toteutus 4](#_Toc531887612)

[4.1 Työmäärien seuranta 4](#_Toc531887613)

[4.2 Liikkeentunnistin 4](#_Toc531887614)

[4.3 Ubuntu Server 18.04 5](#_Toc531887615)

[4.3.1 Basic configuration 5](#_Toc531887616)

[4.3.2 Palvelut 5](#_Toc531887617)

[4.3.3 Tietoturva 6](#_Toc531887618)

[5 Datan visualisointi 9](#_Toc531887619)

[6 Pohdinta 10](#_Toc531887620)

[6.1 Kohdatut ongelmat 10](#_Toc531887621)

[6.1.1 Ubuntu Server 10](#_Toc531887622)

[6.2 Parannukset ja lisättävät 11](#_Toc531887623)

[6.2.1 Ubuntu Server 11](#_Toc531887624)

[7 Lähteet 12](#_Toc531887625)

# Johdanto

Projektin tarkoituksena on luoda toimiva IoT-järjestelmä, joka käyttää monipuolisesti IoT-sovelluksissa käytettäviä tekniikoita ja laitteita.

Projektin aiheeksi valittiin kulunvalvontajärjestelmä, jossa seurataan käyttäjien kantamia RuuviTag-sensoreita sekä järjestelmän liikkeentunnistinta. Käyttäjistä kerättävä data laitetaan talteen tietokantaan ja saataville verkkopalvelimelle.

# Teoria

## Bluetooth

Laitteiden väliseen langattomaan viestintään käytetty protokolla, jossa data lähetetään 2,4 GHz taajuusalueella. Bluetooth yhteyden kantama vaihtelee laitteesta riippuen metristä satoihin metreihin (Radio Versions)

## MQTT

MQTT on julkaisija-lähettäjä –mallilla toimiva protokolla tiedonvälitykseen. Julkaisija(publisher) lähettää kerätyn datan Välittäjälle(Broker). Välitettävä data on järjestetty hierarkisesti, jolloin tilaaja voi tilata joko yksittäisen tiedon, tai tietoa yleisemmin. Välittäjä huolehtii tiedon lähettämisestä kaikille aiheen tilanneille Tilaajille(Subscriber). (MQTT Version 5.0)

## JSON

JavaScript Object Notation tai JSON on avoimen standardin tiedonvälitys formaatti, joka lähettää tiedon luettavassa muodossa avain-arvo –pareina. (Introducing JSON)

## RuuviTag

RuuviTag on avoimen lähdekoodin anturijärjestelmä, joka sisältää kiihtyvyys, lämpötila, ilmankosteus ja ilmanpaine antureita. RuuviTag lähettää keräämänsä datan Bluetooth-yhteyden yli JSON-muodossa lähetyksiä kuunteleville laitteille. (What Is RuuviTag?)

## Ubuntu Server 18.04

Ubuntu Server on avoimen lähdekoodin Linux jakelupaketti, jonka on kehittänyt Canocial monien eri ohjelmoijien kanssa ympäri maailmaa. Ensimmäinen Ubuntu Server on julkaistu vuonna 2010 ja uusin 18.04 versio on julkaistu vuonna 2018. Ubuntu Serveriä voi käyttää niin verkkosivujen ylläpitoon, tiedostopalvelimena tai vaikkapa pilvipalveluna. (TechRepublic, 2017)

# Suunnitelma

Käyttäjien seurantaan käytettiin RuuviTag-sensoreita, jotka mittaavat lämpötilaa, ilmanpainetta, ilmankosteutta ja kiihtyvyyttä. Sensorit lähettävät datan Bluetooth-yhteyden yli Raspberry Pi 3+, joka toimii kontrollerina sensoreille. Raspberry Pi :hin on kiinnitetty myös liikkeentunnistin, jonka dataa mitataan RuuviTagien rinnalla.

Datan lähettämiseen eteenpäin käytetään MQTT-protokollaa. Raspberry toimii tässä toteutuksessa sekä MQTT julkaisija, että välittäjänä. RuuviTag lähettää dataa JSON-formaatissa, joka pakataan uudestaan Raspberryn toimesta ja lähetetään eteenpäin MQTT-viestejä tilanneelle palvelimelle

Dataa vastaanottamaan on laitettu Ubuntu Server 16.04 verkkopalvelin, johon on asennettu MySQL-tietokanta tiedon tallennusta varten. Palvelimella toteutetaan datan visualisointi ja esittely verkkopalvelussa.

Mahdollisina lisäominaisuuksina toteutetaan liikkeentunnistimella aktivoituva mittaus, verkossa näkyvän dashboardin ominaisuuksien laajentaminen ja järjestelmän äänitoiminnot.

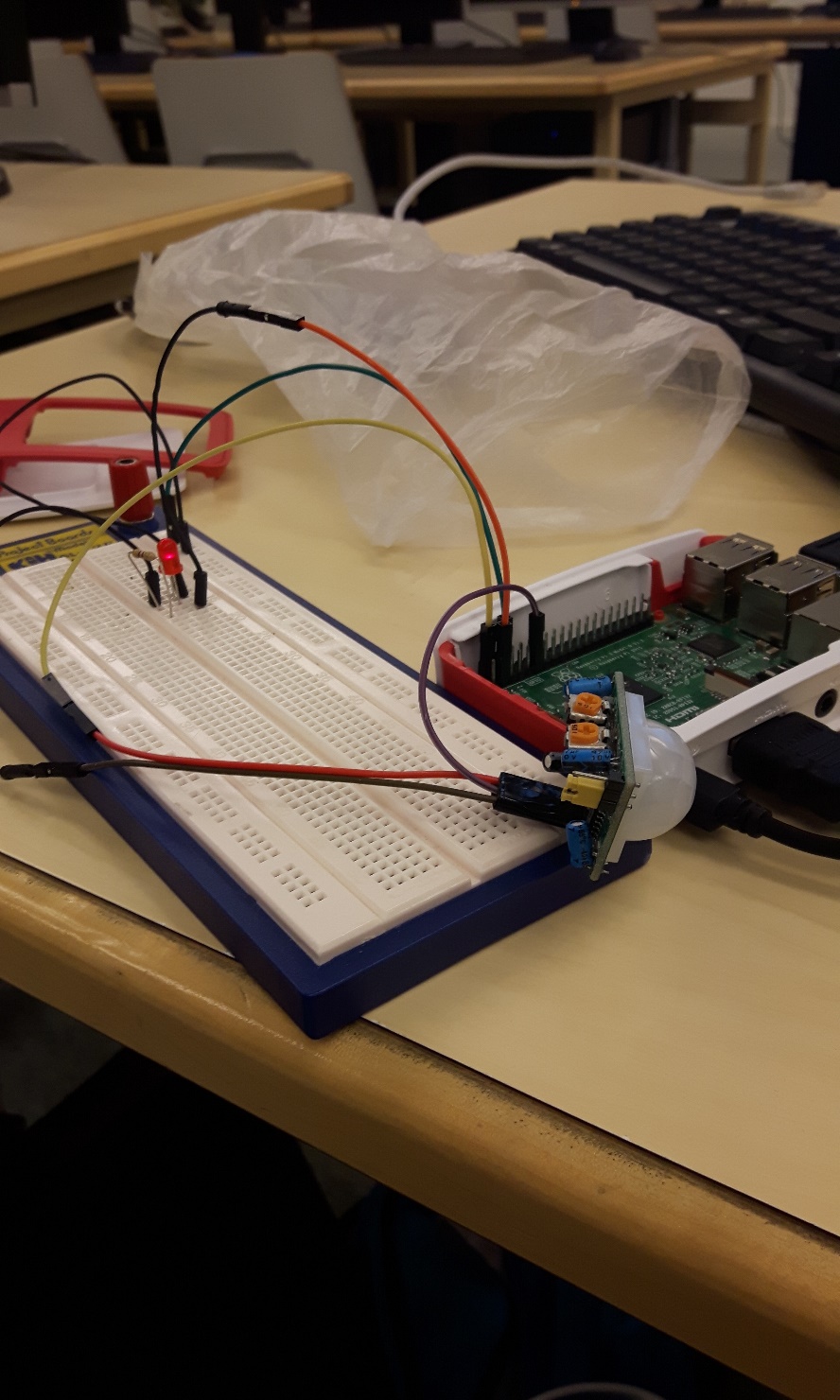
# Toteutus

Työ toteutettiin pääsääntöisesti viikoittaisten oppituntien aikana ryhmässä ja vapaa-aikana yksittäin. Ryhmä piti kirjaa työtehtävistä ja materiaaleista githubissa, laitteiden muistissa olevilla työlistoilla sekä pitämällä yhteyttä ryhmän omalla slack-kanavalla.

## Työmäärien seuranta

## Liikkeentunnistin

Liikkeentunnistimessa ei ollut normaaleja merkintöjä ja osa komponenteista oli valmiiksi vääntyneitä. Testauksen aikana huomattiin, että tunnistin oli viallinen ja signaali oli aina ”high” asennossa. Viallista liikkentunnistusta ei voitu käyttää projektissa, joten sen toiminnallisuuksista luovuttiin.



Kuvio 1 Liikkeentunnistimen testausta

## Ubuntu Server 18.04

Ubuntu Serveriä käytetään työssä palvelimena johon data Raspberry Pi:stä lähetetään ja jossa se käsitellään. Labranetiltä oli tarjolla CentOS 7 sekä Ubuntu Serveriä ja päädyimme Ubuntu Serveriin, koska Ubuntustä löytyi valmista kokemusta ennestään sekä Ubuntu on yksi yleisimmistä Linux-distribuutioista palvelintekniikassa ja täten siihen on helposti löydettävissä dokumentaatiota ja ohjeita palveluiden pystyttämiseen ja hallitsemiseen. (W3Techs, 2018)

### Basic configuration

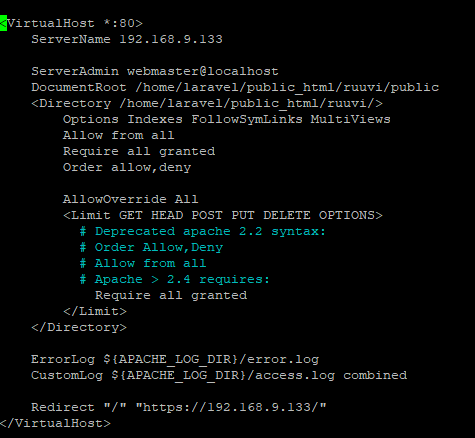
Palvelimelle on asetettu kiinteä IP-osoite 192.168.9.133 ja se toimii JAMK:in Labranetissä sisäisesti. Palvelin on voimassa tähän tietoon tämän vuoden loppuun saakka.

### Palvelut

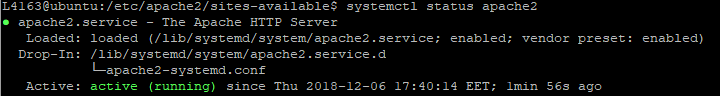
Palvelimelle on asennettu Linux LAMP, joka sisältää Apache web-serverin, MySQL- tietokannan sekä PHP:n.

#### Apache

Apache web-server on tällä hetkellä käytössä ja toimii porteissa 80 sekä 443, jossa pyörii Laravel. Laravelin VirtualHost-tiedostoon on lisätty konfiguraatio, joka ohjaa liikenteen suoraan 80 portista suojattuun 443 porttiin siten, että suojaamatonta yhteyttä ei pääse Laraveliin muodostamaan. (kuvio 2)



kuvio 2 laravel.conf- tiedosto



kuvio Apache-palvelun tiedot

#### MySQL

MySQL-tietokantaa käytetään palvelimella vastaanottamaan ja säilyttämään dataa, jota Raspberry Pi siihen lähettää. TÄYDENNYSTÄ

#### PHP

TÄYDENNYSTÄ

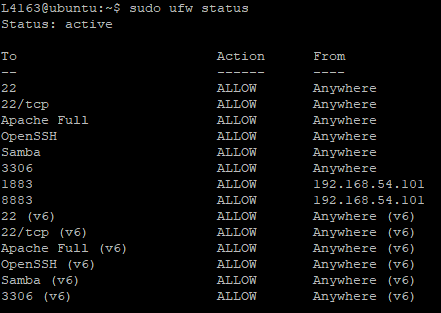
### Tietoturva

#### Käyttäjähallinta

Jokaiselle ryhmäläiselle on luotu henkilökohtaiset tunnukset palvelimen hallintaan. Ryhmän jäsenet on lisätty wheel-ryhmään, joten heillä on administrator-oikeudet palvelimelle suorittaa komentoja. Root sekä Administrator käyttäjien salasanat on generoitu 100-merkkisiksi, jotta niitä Bruteforce- hyökkäyksellä saada selville.

#### Palomuuri

Palomuurissa on seuraavanlainen konfiguraatio:

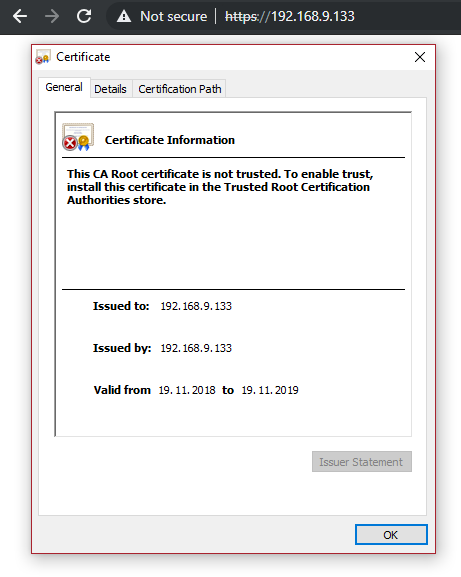


kuvio 4 Palvelimen palomuuri

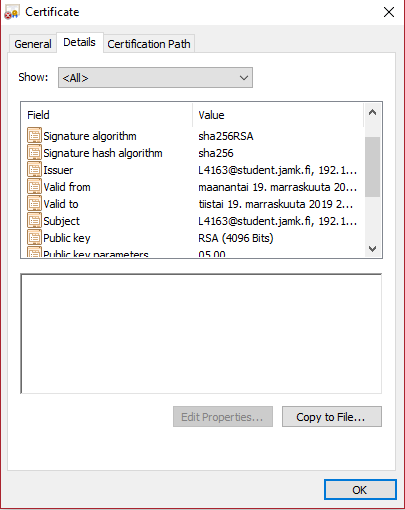
Palomuuri on toteutettu ufw:tä käyttäen, koska se tarjoaa tarvittavat ominaisuudet meidän käyttöömme. Tällä hetkellä portteja on auki Apachelle, OpenSSH:lle, MQTT:lle, SMB:lle sekä MySQL:lle. MQTT-yhteys on sallittu pelkästään Raspberry Pi:n IP-osoitteesta.

#### HTTPS

Palvelimelle on konfiguroitu HTTPS-yhteys Laravelin hallintaan (kuvio 5 ,kuvio 6) . Sertifikaatti on itsekirjoitettu, koska palvelimella ei ole pääsyä julkiseen ulkoverkkoon. Sertifikaatin private key:tä säilytetään palvelimella kansiossa, johon ei ole oikeuksia kuin root-käyttäjällä.



kuvio 5 Itsekirjoitetun sertifikaatin tietoa



kuvio 6 Itsekirjoitetun sertifikaatin tietoa

# Datan visualisointi

Tarkoituksena on käyttää kerättyä dataa ja visualisoida se jotenkin, jolla näkisi esimerkiksi käyttöaikoja eri päivinä ja kellonaikoina. Pohjana käytetään Google graphs -kaavioilla. Se toimii php:lla sekä javascriptillä, jolla saa dataa hyvin yksinkertaisesti taulukoiksi ja kaavioiksi.

Taulukot oisi tarkoitus laittaa yksinkertaiselle html sivulle. Mikäli isompi käyttötarve ilmenee paremmalle käyttöliittymälle, sellainen voidaan rakentaa.

Ainakin seuraavanlaista tietoa haluttaisiin saada tietokannasta ulos:

-Käyttömäärät eri päivinä

-Eri kellonaikojen käyttömäärät

# Pohdinta

## Kohdatut ongelmat

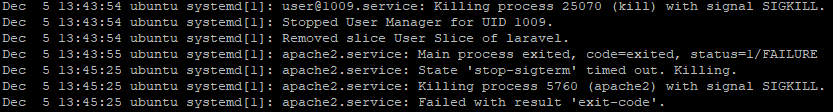
### Ubuntu Server

Ubuntu Serverin kanssa työskentely oli haastavaa, mutta erittäin opettavaista. JAMK:in Linux Server kurssilla on käyty CentOS-distribuutiota, niin jotkin komennot oli haettava googlesta uudestaan.

Lähes jokainen konfiguraatio, jota tehtiin ei mennyt ensimmäisellä kerralla purkkiin. Jokainen konfiguraatio saatiin kuitenkin toimimaan. Suurimmat ongelmat tuli Apachen ja palomuurin kanssa.

Palomuuri oli aluksi helppo laittaa kasaan. Kurssin loppuvaiheilla, kun dokumentaatiota alettiin tekemään, Pekka huomasi ylimääräisen portin jota enää ei tarvittu. Portti suljettiin ja tämän jälkeen kaikki yhteydet palvelimelle pingistä lähtien. Labrainsinöörit nollasivat palomuurin ja säännöt rakennettiin uudestaan ja sama toistui. Saman tempun jälkeen kokeiltiin laittaa pelkkä SSH-yhteys auki, mutta vieläkin sama toistui. Asiaan saatiin labrainsinööreiltä vinkki, että netfilter-persistent jota käytetään sääntöjen tallentamiseen aiheuttaa ongelmaa. Otettiin kyseinen parametri pois käytöstä, käynnistettiin palvelin uudestaan ja tämän jälkeen palomuuri taas toimi normaalisti.

Apachen ongelma on ollut siinä, että se epäonnistuu itsekseen noin kerran viikossa epäsäännöllisesti. Apachen konfiguraatio on kuitenkin oikein sekä se lähtee aina päälle ilman virhekoodia, kun sen käynnistää uudelleen. Lokitiedostoja tarkastelemalla pieni epäilys on siinä, että Laravel saattaisi aiheuttaa ongelmaa. Asiaa kuitenkin tutkiessa alkoi umpikuja tulla vastaan ja tätä ei saatu korjattua kurssin loppuun mennessä.



kuvio 7 Ote syslog-tiedostosta kun Apache on kaatunut

SMB:n pystyttämisessä oli myös pieniä ongelmia, mutta tämä ratkesi perinteisellä poista kaikki ja rakenna uudestaan tyyppisellä metodilla ja on sen jälkeen toiminut ongelmitta.

## Parannukset ja lisättävät

### Ubuntu Server

Jotta palvelimesta olisi tullut ”täydellinen”, siitä pitäisi korjata ongelmat Apachen kanssa. Tämä vaatisi hurjaa määrää testaamista ja paneutumista. Lisäksi palvelimelle olisi hyvä tehdä full update, mutta se on jätetty tässä pois, ettei kurssin viimeisillä metreillä mitään mene kriittisesti rikki.

Tietoturvan osalta MQTT-yhteys suunniteltiin heitettävän TLS-salauksen päälle, mutta samoista aikataulusyistä tämä jätettiin toteuttamatta. Tätä voidaan perustella myös sillä, että kulunvalvonta toimii yleensä sisäverkossa, joten ulkopuolisen tunkeutujan riski on hieman pienempi kuin jos se liikennöisi ulkoverkossa. Sisäverkkoa voi myös koventaa tarvittaessa sertifikaattipalvelimella ja niin edelleen.

Myös kun palvelu on suurin piirtein valmis, sille olisi hyvä tehdä täysivaltainen penetraatiotesti käyttäen esimerkiksi Kali-Linuxia. Tällä tavoin asiat joita ei konfiguraation aikana tullut huomatuksi tulee parhaiten esiin ja näillä tiedoilla palvelimesta saataisiin entistäkin turvallisempi.

# Lähteet

Radio Versions. N.n. Artikkeli Bluetoothin sivuilla. Viitattu 16.11.2018 <https://www.bluetooth.com/bluetooth-technology/radio-versions>

MQTT Version 5.0. N.d. Artikkeli Oasis-säätiön sivuilla. Viitattu 16.11.2018 <http://docs.oasis-open.org/mqtt/mqtt/v5.0/cos01/mqtt-v5.0-cos01.html>

Introducing JSON. Kirjoitus JSON:in sivuilla. N.d. Viitattu 16.11.2018 <https://www.json.org/>

What Is RuuviTag?. N.d. Esittely RuuviTagin sivuilla. Viitattu 16.11.2018 <https://ruuvi.com/ruuvitag-specs/>

Ubuntu Server: A cheat sheet. Artikkeli TechRepublicin sivustolla. Viitattu 23.11.2018

<https://www.techrepublic.com/article/ubuntu-server-the-smart-persons-guide/>

Usage statistics and market share of Linux for websites. Artikkeli W3Techsin sivuilla. Viitattu 6.12.2018

https://w3techs.com/technologies/details/os-linux/all/all