IoT-järjestelmän toteutus

Harjoitustyö

Antti Kettunen

Hannu Oksman

Pekka Sivusuo

Antti Tarvainen

Saku Tupala

Harjoitustyö

Joulukuu 2018

Tekniikan ja liikenteen ala

Tieto- ja viestintätekniikan koulutusohjelma

Sisällys

[1 Johdanto 3](#_Toc532763437)

[2 Käsitteet 3](#_Toc532763438)

[2.1 Bluetooth 3](#_Toc532763439)

[2.2 MQTT 3](#_Toc532763440)

[2.3 JSON 3](#_Toc532763441)

[2.4 RuuviTag 4](#_Toc532763442)

[2.5 Ubuntu Server 18.04 4](#_Toc532763443)

[3 Suunnitelma 4](#_Toc532763444)

[4 Toteutus 5](#_Toc532763445)

[4.1 Työmäärien seuranta 5](#_Toc532763446)

[4.2 Datan reitti 5](#_Toc532763447)

[4.3 Liikkeentunnistin 6](#_Toc532763448)

[4.4 Ubuntu Server 18.04 7](#_Toc532763449)

[4.4.1 Basic configuration 7](#_Toc532763450)

[4.4.2 Palvelut 7](#_Toc532763451)

[4.4.3 Tietoturva 10](#_Toc532763452)

[5 Pohdinta 13](#_Toc532763453)

[5.1 Kohdatut ongelmat 14](#_Toc532763454)

[Lähteet 18](#_Toc532763455)

**Kuviot**

[Kuva 1. Liikkeentunnistimen testausta 7](#_Toc532763456)

[Kuva 2. IoT-kokonaisuus 8](#_Toc532763457)

[Kuva 3. laravel.conf-tiedosto 9](#_Toc532763458)

[Kuva 4. Apache-palvelun tiedot 9](#_Toc532763459)

[Kuva 5. IoT-tietokannan rakenne 10](#_Toc532763460)

[Kuva 6. Palvelimen palomuuri 11](#_Toc532763461)

[Kuva 7. Itsekirjoitetun sertifikaatin tietoa 12](#_Toc532763462)

[Kuva 8. Itsekirjoitetun sertifikaatin tietoa 13](#_Toc532763463)

[Kuva 9. Ote syslog-tiedostosta, kun Apache on kaatunut 15](#_Toc532763464)

# Johdanto

Projektin tarkoituksena oli 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. Emme kuitenkaan saaneet liiketunnistinta toimimaan.

# Käsitteet

## 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 n.d.)

## MQTT

MQTT on julkaisija-lähettäjä –mallilla toimiva protokolla tiedonvälitykseen. Julkaisija (publisher) lähettää kerätyn datan välittäjälle (broker). Välitettävä data on järjestetty hierarkkisesti, jolloin tilaaja voi tilata joko yksittäisen tiedon, tai tietoa yleisemmin. Välittäjä huolehtii tiedon lähettämisestä kaikille aiheen tilanneille tilaajille (subscriber). (MQTT Version 5.0 n.d.)

## JSON

JavaScript Object Notation (JSON) on avoimen standardin tiedonvälitysformaatti, joka lähettää tiedon luettavassa muodossa avain-arvo –pareina. (Introducing JSON n.d.)

## 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? N.d.)

## 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 sovelletaan RuuviTag-sensoreita, jotka mittaavat lämpötilaa, ilmanpainetta, ilmankosteutta ja kiihtyvyyttä (x-, y- ja z-akselit sekä niistä laskettu vektori). Sensorit lähettävät datan Bluetooth-yhteyden yli Raspberry Pi 3+:lle, joka toimii kontrollerina sensoreille.

Datan lähettämisessä ja vastaanottamisessa käytetään MQTT-protokollaa. Raspberry toimii tässä toteutuksessa sekä MQTT-julkaisijana että välittäjänä. RuuviTag lähettää dataa JSON-formaatissa ja tämä lähetetään Raspberryn toimesta eteenpäin MQTT-viestejä tilanneelle palvelimelle.

Dataa vastaanottaa Labranetissä oleva virtuaalikone. Palvelimella toteutetaan datan visualisointi ja esittely verkkopalvelussa.

Mahdollisina lisäominaisuuksina toteutetaan liikkeentunnistimella aktivoituva mittaus, verkkopalvelun ominaisuuksien laajentaminen ja järjestelmän äänitoiminnot. Yksi mahdollisuus tunnistautumiseen sekä kirjautumiseen olisi opettaa neuroverkolle meidän äänillämme muutama sana.

Datan visualisointi

Tarkoituksena on visualisoida esimerkiksi sensoreista saadut lämpötilat ja läsnäolo päivinä ja kellonaikoina. Kaavioiden piirto toteutetaan PHP:llä ja JavaScript:llä toimivalla Google Graphs -kirjastolla.

Taulukot olisi 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

# Toteutus

Työ toteutettiin pääsääntöisesti viikoittaisten oppituntien aikana ryhmässä ja vapaa-aikana yksittäin tai pareittain. Osa ryhmästä piti osan aikaa kirjaa työtunneista. Materiaalien säilytys ja versioidenhallinta hoidettiin Rasberry:lla, virtuaalikoneella ja GitHubissa. Yhteyttä pidettiin ryhmän omalla Slack-kanavalla ja koululla.

## Työmäärien seuranta

Sivusuo ja Kettunen pitivät kirjaa työtunneista ja taulukko on GitHub:ssa.

## Datan reitti

Tiedon siirto RuuviTagiltä Raspberry Pi:lle tapahtuu lyhyen matkan Bluetoothin välityksellä (Bluetooth Low Energy, BLE), Pi ottaa datan vastaan JSON-muodossa, luo MQTT-aiheen ja aiheeseen viestin lähellä olevien RuuviTag:en datasta 5 sekunnin välein.

Virtuaalikoneella tilataan Pi:n MQTT-aihe ja aina kun aiheeseen on saapunut uusi viesti, niin se otetaan vastaan, puretaan JSON muodosta ja tallennetaan tietokantaan.

MQTT:n hallinnointiin on käytetty Eclipse Paho MQTT Python kirjasto. Paho tarjoaa luokan, joka sallii MQTT välittäjään yhdistämisen viestin lähettämistä, aiheiden tilausta ja viestien vastaanottoa varten (Fersing & Light 2018). Toteutimme myös MQTT-autentikoinnin, aiheen tilaamiseen tarvitsee voimassaolevat tunnukset (määritellään aiheen lähettämisessä).

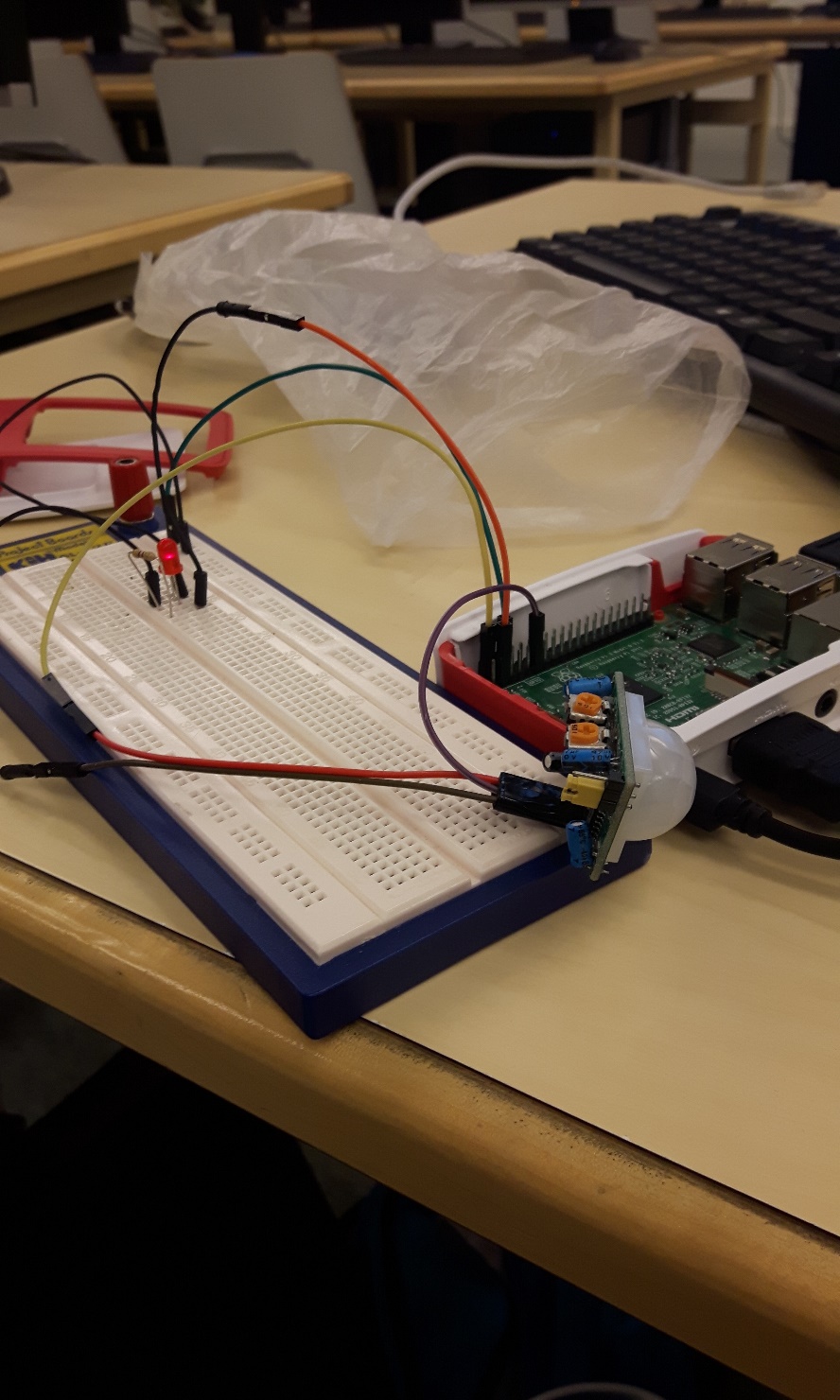
Datan tallentamiseen tietokantaan on käytetty Peewee ORM (Object-Relational Mapping) (Leifer n.d.). Peewee sallii tietokannan taulujen tallentamisen objekteiksi, joiden avulla tietokantaan tallentaminen onnistuu helposti ilman raakojen kyselyiden valmistelua. Haittana on hitaus normaaleihin kyselyihin verrattuna, mutta tämänkaltaisessa käytössä Peewee:n käyttö ei hidasta toimintaa juuri ollenkaan.

MQTT lähetys, kuuntelu ja tietokantaan tallennus skriptien suoritus uudelleenkäynnistyksen jälkeen toteutettiin shell skriptillä. Shell skripti suorittaa MQTT skriptit aina käynnistyksen jälkeen 30 sekunnin viiveellä ja skriptit jäävät pyörimään taustaprosessina (daemon).

Tietokannan dataan pääsee käsiksi Laravel-PHP-ohjelmistokehyksellä toteutetulla REST API -rajapinnallamme tai yhdistämällä suoraan tietokantaan käyttämällä MYSQL:iin luodun etäkäyttäjän tunnuksia. Etäkäyttäjällä on vain lukuoikeudet tietokannan Data-tauluun.

## Liikkeentunnistin

Liikkeentunnistimessa ei ollut normaaleja merkintöjä ja osa komponenteista sekä pinneistä olivat valmiiksi vääntyneitä. Testauksen aikana huomattiin, että tunnistin oli viallinen ja signaali oli aina ”high” asennossa. (Ks. kuva 1.) Viallista liikkeentunnistusta ei voitu käyttää projektissa, joten sen toiminnallisuuksista luovuttiin.



Kuva 1. Liikkeentunnistimen testausta

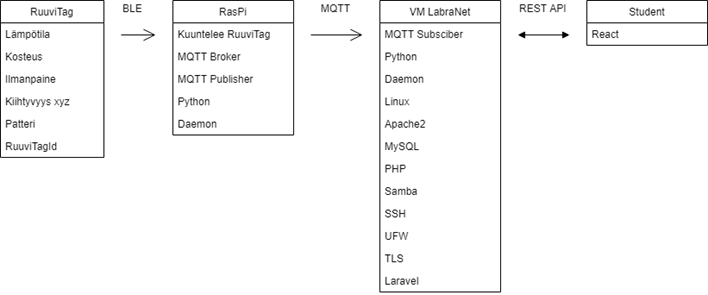
## Ubuntu Server 18.04

Ubuntu-palvelinta käytetään virtuaalikoneella, johon data Raspberry Pi:stä lähetetään ja jossa se käsitellään. Labranet tarjosi CentOS 7 sekä Ubuntu Server ja päädyimme Ubuntu Serveriin, koska Ubuntusta löytyi valmista kokemusta ennestään. Lisäksi 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.

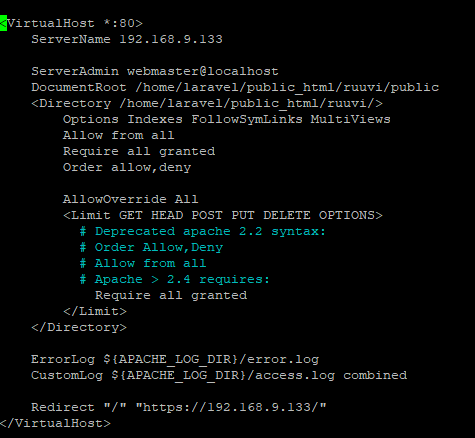
### Palvelut

Palvelimelle on asennettu Linux LAMP, joka sisältää Apache web-serverin, MySQL- tietokannan sekä PHP: n. Asensimme myös muita palveluita, kuten Samban. (Ks. kuva 2.)

Kuva 2. IoT-kokonaisuus

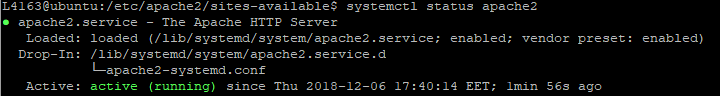
Apache

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. (Kuvassa 3 laravel.conf-konfiguraatiotiedosto, toiseksi alimmalla rivillä uudelleenohjaa kaiken https-yhteyteen.)



Kuva 3. laravel.conf-tiedosto

Apache-palvelimen tilan voi tarkistaa komennolla systemctl status apache2. (Ks. kuva 4, komennon tulostama syöte.)

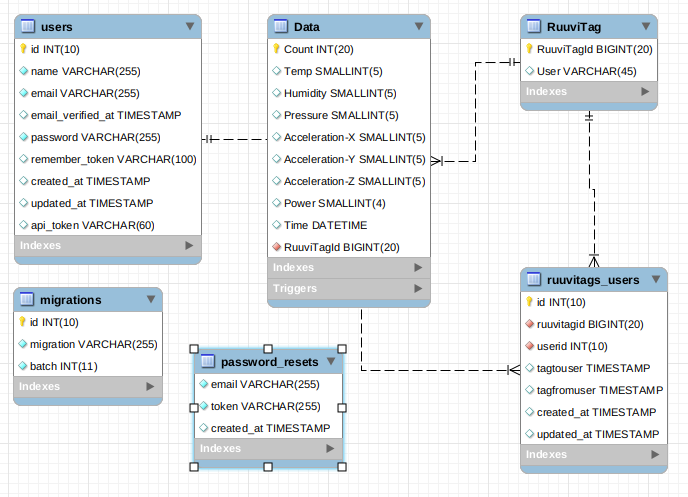


Kuva 4. Apache-palvelun tiedot

MySQL

Toteutuksessa käytetään MySQL-tietokantaa. IoT-toteutuksen kannalta tärkeimmät taulut ovat RuuviTag ja Data. Rest API:a varten lisäsimme taulut users, ruuvitags\_users ja password\_resets. (Ks. kuva 5.). Migrations taulu on Laravelin migraatioita varten.

* RuuviTag-taulu sisältää käyttäjänimen ja käyttäjän RuuviTag:n MAC-osoitteen muunnettuna bigint-tietotyyppiin (RuuviTag-taulun primary key)
* Data-taulussa säilytetään RuuviTag:stä saadut mittaukset
* Users, ruuvitags\_users ja password\_resets tauluja käytetään Rest API:ssa käyttäjätoimintoihin.



Kuva 5. IoT-tietokannan rakenne

Laravel REST API

Käytimme Oksmanin ja Tarvaisen Web-palvelinohjelmointi-opintojaksolle tehtyä rajapintaa. (Lisätietoja rajapinnan toteutuksesta ks. Oksman, Seppälä & Tarvainen 2018.)

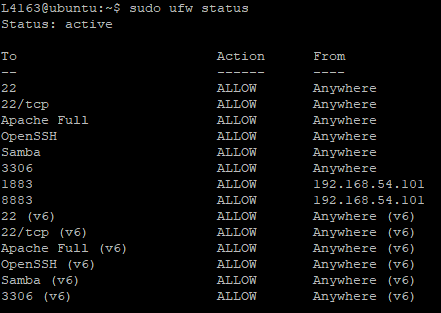
### Tietoturva

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 ei voi saada Bruteforce- hyökkäyksellä selville.

Palomuuri

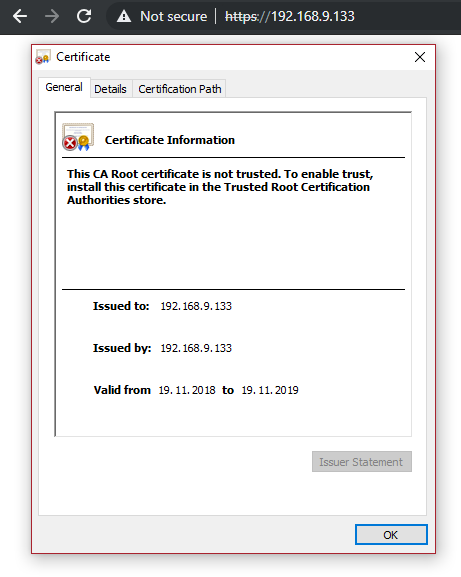
Palomuuri on toteutettu ufw:tä käyttäen, koska se tarjoaa tarvittavat ominaisuudet meidän käyttöömme. Tällä hetkellä portteja on auki Apachelle, OpenSSH:lle, MQTT:lle, SMB:lle sekä MySQL:lle. MQTT-yhteys on sallittu pelkästään Raspberry Pi:n IP-osoitteesta. (Ks. kuva 6, palomuurin konfiguraatio.)



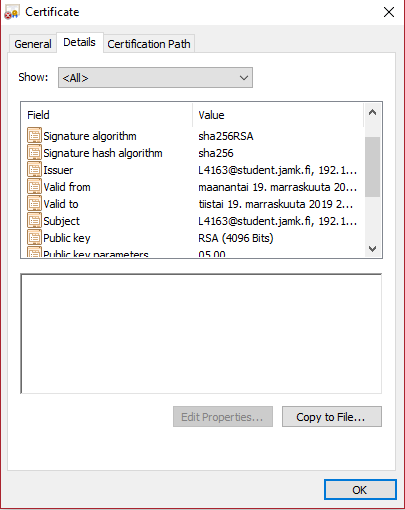
Kuva 6. Palvelimen palomuuri

HTTPS

Palvelimelle on konfiguroitu HTTPS-yhteys Laravelin hallintaan (Ks. kuva 7 ja kuva 8.). Sertifikaatti on kirjoitettu itse, koska palvelimella ei ole pääsyä julkiseen ulkoverkkoon. Sertifikaatin private key -avainta säilytetään palvelimella kansiossa, johon ei ole oikeuksia kuin root-käyttäjällä.



Kuva 7. Itsekirjoitetun sertifikaatin tietoa



Kuva 8. Itsekirjoitetun sertifikaatin tietoa

React-sovellus

RuuviTag-sensoreista saadun datan visualisointi on toteutettu Oksmanin ja Tarvaisen Web-ohjelmointi-opintojaksolle luomalla React JavaScript-kirjastolla toteutetulla web-sovelluksella. (Lisätietoja sovelluksen toteutuksesta ks. Oksman, Seppälä & Tarvainen 2018.)

# Pohdinta

Toteutimme toimivan IoT-kokonaisuuden, mutta olisimme halunneet tehdä enemmän elektroniikkaan ja sensoreihin liittyen. Yksi haaste oli, ettemme ole vielä tehneet elektroniikan ja sulautetun ohjelmoinnin opintojaksoja. Olemme kuitenkin erittäin tyytyväisiä ja ylpeitä lopputuloksesta.

Olisi ollut hyvä pitää alusta asti kirjaa työtunneista, niin olisi jälkikäteen voinut todentaa mihin toimintoihin ja tehtäviin aika kului. Siitä olisi myös hyvin selvinnyt kuka teki ja kuinka paljon töitä. Käytämme tuntikirjanpitoa tulevilla toteutusopintojaksoilla.

## Kohdatut ongelmat

Kohtasimme paljon haasteita, joiden selvittäminen vei paljon aikaa, mutta olivat opettavaisia. Nyt tiedämme enemmän teknologioista ja hahmotamme paljon paremmin, miten IoT-kokonaisuus toimii ja millainen rakenne sillä voi olla.

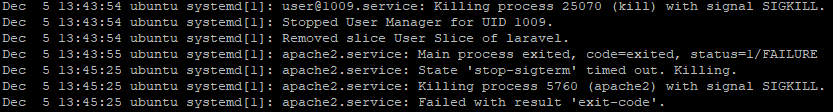
Ubuntu Server

Ubuntu Server:n kanssa työskentely oli haastavaa, mutta erittäin opettavaista. Sivusuo on käyttänyt JAMK:n Linux Server kurssilla CentOS-distribuutiota, niin jotkin komennot oli haettava Googlesta uudestaan. Muut ryhmäläiset ovat asentaneet, konfiguroineet ja käyttäneet kaikkia palveluita muilla opintojaksoilla. Palvelinopintojaksot voisivat olla pakollisia ohjelmisto-opiskelijoillekin.

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. (Ks. kuva 9.) Asiaa kuitenkin tutkiessa alkoi umpikuja tulla vastaan ja tätä ei saatu korjattua kurssin loppuun mennessä.



Kuva 9. 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.

Ubuntu Server -parannukset

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.

RuuviTag:n Python-kirjaston käyttö

Käytimme pohjana Johdatus teolliseen Internetiin –opintojaksolle tehtyä RuuviTag-sensoreiden kuunteluun käytettyä skriptiä. Karsimme siitä tarpeettoman ja refaktoroimme tähän toteutukseen soveltuvan version.

Aluksi käytimme sensoridatan keräämiseen RuuviTag-kirjaston sensor.update-metodia, joka kuuntelee sensoreilta tulevia päivityksiä. Mutta jos Raspberryn lähellä ei ollut yhtään sensoria, niin skriptin suoritus ei mennyt eteenpäin eikä myöskään jatkunut, kun lähelle toi yhden sensoreista.

Vähensimme ongelmaa käyttämällä UNIX:n SIGALRM-signaalia. Käytimme sitä niin, että jos sensor.update() ei palauta mitään viiteen sekuntiin, niin sen säie lopeetaan, jolloin ohjelman suoritus jatkui.

Signaaliratkaisukaan ei lopulta toiminut, koska jostain syystä skripti jäi silti odottamaan päivitystä sensoreilta. Onneksi löysimme RuuviTag:n dokumentaatiosta asynkronisen get\_datas-metodin, johon lähetetään parametreina itse tehty funktio (se ottaa sensoridatan ja julkaisee sen MQTT:lla) ja sensorin MAC-osoite.

MQTT-kuuntelija

Virtuaalipalvelimen MQTT-kuuntelijan skripti jäi jumiin, jos MQTT-lähetys skripti myös jäi jumiin. Tämä johtui siitä, että Paho-kirjaston skripti uudelleenyhdisti automaattisesti MQTT-välittäjään, mutta ei tilannut uudestaan aihetta. Skripti siis näkyi sen tilaa tarkastellessa toimivana, mutta ei enää saanut uusia viestejä aiheesta. Tämä korjaantui siirtämällä skriptin subscribe-metodi onconnect-metodin sisälle, joka suoriutuu aina skriptin yhdistäessä uudestaan MQTT-välittäjään.

Tietokannan Data-taulu

Data-taulun Count-primarykey-kenttä määriteltiin autoincrement ja smallinteger kentäksi, tämä aiheutti sen, ettei tietokantaan pystynyt enää Count-kentän noustessa lukuun 32,767 tallentamaan dataa. Onneksi tajusimme tämän vian nopeasti ja pääsimme muokkaamaan Count-kentän integer tyypiksi, jotta muisti ei taas loppuisi kesken.

Virtuaalikoneen alhaiset resurssit

Kun Data-taulussa yli satatuhatta tietuetta, niin kaikkea dataa ei enää saanut haettua Laravel-rajapinnalla. Apache2-virhelokeista selvisi, että php.ini-tiedostossa määritetty PHP:n muistinkäyttöraja oli ylittynyt. Virtuaalikoneella ei kuitenkaan ole paljoakaan keskusmuistia vapaana, joten emme voineet nostaa PHP:n muistirajaa. Teimme nopean muutoksen rajapintaan ja nyt se palauttaa vain tuhat tietuetta kerralla.

Lähteet

Fersing, P & Light, R. 2018. Paho MQTT -projektin verkkosivut. Viitattu 5.12.2018. <https://pypi.org/project/paho-mqtt/>.

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

Leifer, C. N.d. Peewee ORM -verkkosivustot. Viitattu 5.12.2018. <http://docs.peewee-orm.com>.

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>.

Oksman, H., Seppälä J. & Tarvainen, A. 2018. ReactIotProject. GitHub-repositorio, jossa dokumentaatio. <https://github.com/atarvainen/reactIoTproject/blob/master/README.md>.

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

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>.

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