Eero Lehtonen

IOT YKSITYISKÄYTÖSSÄ

Tietojenkäsittelyn koulutusohjelma

2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

IOT YKSITYISKÄYTÖSSÄ

Lehtonen, Eero
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2018
Ohjaaja: Hentunen, Ilmari
Sivumäärä: 29
Liitteitä: 0

Asiasanat: IoT, Esineiden Internet, automaatio, tietoturva

Tämän opinnäytetyön tarkoituksena on esitellä Internet of Thingsin toimintaa kuluttajan näkökulmasta katsottuna. Työn alussa käyn käsitettä läpi yleisellä tasolla.

Internet of Thingsin toiminta on jaettu kahteen osaan, jotka ovat kuluttaja-IoT, sekä teollisuuden IoT. Työssä tutkittiin millä laitteilla ja yhteystekniikoilla voidaan toteuttaa kodin automaation ratkaisuja. Olen käsitellyt pilvipohjaisten alustojen ominaisuuksia päällisin puolin, tutkimatta tarkemmin niiden toimintaa käytännössä.

Internet of Thingsin ominaisuuksiin sisältyy paljon hyötyjä, mutta myös haittapuolia, joita olen pyrkinyt selvittämään. Merkittävin uhka on tietoturva. Työssä käy ilmi minkälaisilla toimilla tavallinen kuluttaja voi parantaa omaa tietosuojaansa.

IOT IN PRIVATE USE

Lehtonen, Eero
Satakunta University of Applied Sciences
Degree Programme in Data Processing
April 2018
Supervisor: Hentunen, Ilmari
Number of pages: 29
Appendices: 0

Keywords: IoT, Internet of Things, automation, data security

The purpose of this thesis was to introduce the actions of the Internet of Things from a consumer's point of view. In the beginning of the work I will explore the concept in general.

Functions of the Internet of Things are divided in two fields, which are consumer-IoT and Industrial IoT. I researched what kind of devices and connection technologies can operate a functional home automation solutions. I have searched the general features of the cloud-based platforms, without further examination of their practical actions.

Internet of Things involves a lot of benefits, but it also contains some disadvantages, which I have tried to sort out. The most significant threat for IoT is data security. In this work I have explaned what kind of actions ordinary consumer can make, to improve their own privacy.
.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön aiheena on IoT yksityiskäytössä. Lyhenne IoT tulee sanoista Internet Of Things. Termin suomenkielinen nimitys on Esineiden Internet. Internet Of Thingsin idea perustuu siihen, että internet-yhteys laajennetaan esineisiin sekä asioihin joita käytämme päivittäin. Tällöin niitä voidaan hyödyntää tehokkaammin, tai niille voidaan kehittää uusia toimintatapoja vanhojen käyttötarkoitusten lisäksi. Internet Of Thingsiä voidaan laajasti hyödyntää teollisuudessa, organisaatioissa sekä yksityisellä tasolla esimerkiksi kotitalouksissa.

Aihealueena IoT on laaja, joten rajasin työn aiheeksi kuluttajalle suunnatut IoT-ratkaisut. Opinnäytetyössä pyrin selvittämään minkälaisia IoT:n ratkaisuja on tällä hetkellä saatavilla kotikäyttöön, eli ns. kuluttajien hyödyksi. Tarkoituksena on tutkia, mitä laitteita voidaan käyttää kodin automaatioratkaisujen totetutuksissa. Perehdyn tällä hetkellä käytössä oleviin yhteystekniikoihin, joilla voidaan luoda yhteyksiä älylaitteiden sekä älyratkaisujen välillä. Olen selvittänyt työssä myös tietoturvan merkitystä aiheeseen liittyen, sillä tietoturva-uhkat koskevat yhtävertaisesti IoT-laitteita, kuin muitakin verkoon kytkettyjä laitteita. Työssä selvitän minkälaisilla asioilla kuluttaja voi omaa tietosuojaansa parantaa.

Valitsin opinnäytetyön tämän aiheen sillä perusteella että se kuulosti kiinnostavalta, mutta itselläni ei sen tarkempaa tietoa aiheesta vielä ollut. Työskentelen elektroniikkaa ja kodintekniikkaa myyvässä yrityksessä, joten sitä kautta osa opinnäytetyön aihealueista on ennestään tuttuja. Tällä opinnäytetyöllä ei ole toimeksiantajaa, eli teen tämän työn tutkimuksellisessa mielessä itseäni kiinnostavaa aihetta kohtaan.

2 IOT YLEISESTI

IoT-teknologia on laaja käsite, koska sitä voidaan hyödyntää monessa eri muodossa. Rakennuksia, liikenneverkkoja, kodinkoneita, kokonaisia kaupunkeja tai jopa ihmiskehoja voidaan yhdistää internetverkkoon. Laitteisiin kytkettyjen sensoreiden ja mikroprosessoreiden avulla voidaan kerätä hyödyllistä dataa ja lähettää sitä muille laitteille. Kerättävä tieto voi olla esimerkiksi liikettä, ääntä, lämpötila-arvoja, sekä useita muita mittausarvoja. Yleisimpiä laitteita joilla tietoa kerätään, ovat tietokoneet, älypuhelimet sekä tabletit. Tällä hetkellä noin 5% laitteista ja esineistä on älylaitteita, eli niissä on elektroniikkaa jolla voidaan kerätä informaatiota omasta tai ympärillä tapahtuvasta toiminnasta. Tietoteknisten komponenttien hinnat ovat laskeneet merkittävästi, ja näin ollen niiden liittäminen jokapäiväisiin laitteisiin on mahdollista. (Swan 2012.)

Yhtenä hyvänä esimerkkinä päivittäin käytettävistä IoT-laitteista voidaan mainita älykello, joka mittaa useita tietoja käyttäjästään. Tällaisia mittausarvoja on esimerkiksi liike, syke ja paikannus. Laitteen mittaama data tallentuu pilvipalveluun käyttäjän tilille, josta tietoja voidaan tarkkailla myöhemmin esimerkiksi yhteenvetona päivän mittaan kerääntyneistä askelista, tai kulutetusta kalorimäärästä.

Kun laitteisiin lisätään älyllisiä komponentteja, voidaan puhua niiden “päivittämisestä”, jolloin niiden käyttöarvo kasvaa saadessaan uusia ominaisuuksia. Verkkoon kytkemisen jälkeen laitteiden on mahdollista keskustella toisten laitteiden kanssa, jonka ansiosta ne pystyvät hyödyntämään tietoa keskenään. Tällöin ne muodostavat yhdessä suurempia älykkäitä kokonaisuuksia. Niiden toimintaa voidaan myös seurata reaaliajassa verkon yli, eli käyttäjä pystyy tarkkailemaan ja hallitsemaan esimerkiksi kotona olevia laitteita etänä. Tätä kutsutaan älykkääksi kodin automaatioksi. Älykkäällä kodin automaatiolla tavoitellaan ensisijaisesti helpotusta arkeen, sekä kustannussäästöjä, ja parempaa turvallisuutta. Nykyisin jo asuintilojen rakennusvaiheessa suunnitellaan näitä asioita pidemmällä tähtäimellä, kustannustehokkaasti ja ennakoiden. (Friedemann & Floerkemeier 2010.)

IOT:n toimintaa on sovellettu jo jonkin aikaa yrityksissä, organisaatioissa, sekä yhteiskunnallisella tasolla. Osa sen toiminnasta on maallikon silmin huomaamatontakin. Tarkemmin asiaa mietittynä se vaikuttaa kuitenkin lähes kaikkialla, kiinteistöjen ja liikenteen valvonnassa, kodintekniikassa sekä kulkuvälineissä. Auton navigaattori, joka saa liikennetiedotuksia internet-verkon kautta. Etäluettava sähkömittari, tai matkapuhelimen avulla päälle kytkettävä saunan kiuas. Tämän kaltaiset elämää helpottavat ratkaisut pohjautuvat IoT-teknologiaan.

3 HISTORIA

Vuonna 1999, teknologian edelläkävijä Kevin Ashton kehitti työpaikallaan Procter & Gamble -nimisessä organisaatiossa idean etäluettavista globaaleista RFID- tunnisteista. Tarkoituksena oli parantaa yrityksen tehokkuutta ja toimitusketjun toimintaa. Tätä ideaa lähti toteuttamaan MIT AutoID laboratorio, joka saikin tukea yhteensä 103 sponsorilta. Kevin Ashton nimesi tällöin projektin nimellä Internet Of Things. Ashtonin mukaan idean tarkoitus on että fyysinen maailma tulisi yhdistymään internetiin globaalisti standardisoiduilla sensoreilla. (Maney 2014)

Vaikka Internet Of Things- termi on keksitty vasta 1999, on jo sitä ennen ollut laitteita jotka toimivat samalla periaattella. Vuonna 1982 Carnegie Mellon yliopistossa oppilaat Mike Kazar, David Nichols, John Zsarnay ja Ivor Durham kehittelivät etäluettavan Coca Cola juoma-automaatin. Nämä IT-alan opiskelijat asensivat Cola-automaattiin mikrokytkimiä, jotka olivat yhteydessä koulun keskustietokoneeseen. Näin oppilaat pystyivät etänä näkemään kuinka paljon juomapulloja oli koneessa jäljellä, sekä kuinka pitkään pullot olivat olleet koneessa josta taas selvisi olivatko ne kylmiä. (Know Your Meme 2010)

Ensimmäiset kodin automaatioon liittyvät toteutukset olivat enemmänkin keksintöjä ja ideoita, kuin älykkäitä toimivia kokonaisuuksia. Kodintekniikkaa on kehitelty 1900-luvun alusta alkaen. Osa näistä on meille jo jokapäiväisessä käytössä tunnettuja laitteita. Näitä keksintöjä ovat mm. moottorikäyttöinen pölynimuri, jääkaapit ja pyykinpesukoneet. Vasta 2000-luvun alussa kodin teknologia on yleistynyt suuremmalla mittakaavalla, pääosin siitä syystä että automaatiolaitteiden hinnat ovat laskeneet kohtuullisiksi kuluttajille. (Hendricks 2014)

Viimeisen kymmenen vuoden aikana teknologian kehitys on ollut huipussaan. Tämä näkyy hyvin esimerkiksi älypuhelinten kehityksessä. Älypuhelimen omistaminen on jo arkipäivää, ja sen avulla voidaan vuorovaikuttaa muiden ihmisten ja laitteiden kanssa. Mobiililaitteiden yhteysnopeudet ovat kasvaneet 3G-, ja 4G-tekniikan myötä. Tietotekniikkavalmistajat ovat onnistuneet rakentamaan yhä pienempiä komponentteja, kuten mikroprosessoreita ja muistipiirejä. Komponenttien koko on ratkaisevassa asemassa, älykkäiden laitteiden suunnittelun ja kehityksen saralla.

4 IOT YKSITYISKÄYTÖSSÄ

Internet Of Thingsin kehityksen aikana on voitu jakaa sen toimintoja eri osa-alueisiin. Pääosin sen käyttö on on kohdistunut teollisuuteen, jossa toimintoja ollaan pystytty tehostamaan tuotannon-, logistiikan- sekä maatalouden aloilla. Tällöin puhutaan IIoT:sta (Industrial Internet Of Things), eli Teollisuuden IoT:sta. Vastikkeena tälle ollaan saatu oma termi CIoT (Consumer Internet of Things), eli Kuluttaja-IoT. Näiden ero perustuu lähinnä käytettäviin laitteisiin ja sovelluksiin. Tarkoitusperä on kuitenkin kummallakin IoT:n osa-alueella sama, halutaan kehittää ja tehostaa toimintaa.

Kuluttaja-IoT:n trendit liittyvät pääosin kodin, sekä jokapäiväisten esineiden automatisointiin, sekä itsensä mittaamiseen. Viimevuosina IoT-laitteiden markkinaosuus kuluttajille on ollut kasvusuuntainen, mutta markkinoiden kehitystä jarruttaa vielä laitteiden hinta, sekä tietoturvallisuuteen liittyvät seikat. Myös osa kuluttajista on vielä sitä mieltä, että IoT-laitteiden käyttö on hankalaa. Toisaalta alan kehitys alkaa olla siinä kääntöpisteessä, jolloin IoT:n tuoma lisäarvo peittoaa sen aiheuttamat haittapuolet.

Kodin automaatiolla tarkoitetaan prosessia, jossa hallitaan kodinkoneita sekä muita kotitalouden laitteita niissä olevien älykomponenttien avulla. Älylaitteiden valikoima on laajentunut viimevuosina merkittävästi, ja uusia laitteita tulee jatkuvasti markkinoille. Näillä on tarkoitus helpottaa käyttäjän perusarkea. Kodin automaatiolaitteita voi olla esimerkiksi ilmastointi, älylukot, älykäs valaistus sekä murtohälyttimet ja palohälyttimet. (Hardik 2017)

Suurin ja merkittävin hyöty IoT-ratkaisuissa on käyttäjämukavuus. Automaattisesti toimivat, tai puhelimella ohjattavat laitteet säästävät aikaa, ja vapauttavat käyttäjän aikaa muihin askareisiin. Älykkäät laitteet maksavat enemmän kuin tavalliset vastaavat laitteet, mutta toisaalta taas säästävät esimerkiksi vesi- ja sähkölaskuissa rahaa. Pidemmällä ajanjaksolla katsottuna se on siis taloudellisesti kannattavaa. Kodin lämmityskuluissa voidaan säästää kytkemällä asunto ylläpitolämmölle kun kotona ei ole ketään, ja lämpötilaa nostetaan kun käyttäjä on palaamassa kotiin. Kodin automaatiolaitteilla voidaan vaikuttaa myös turvallisuuteen. Älylaitteet lisäävät turvallisuuden vaikutelmaa, koska ne valvovat jatkuvasti mitä asunnossa tapahtuu. Asunto jossa valot syttyvät automaattisesti pimeän tultua päälle, on epätodennmäköisempi kohde myös murtautujalle. Murtautumistilanteessa käyttäjä saa informaation tilanteesta puhelimeen, ja järjestelmä pystyy ilmoittaa murrosta suoraan vartiointiyritykselle.
(Meola 2016)

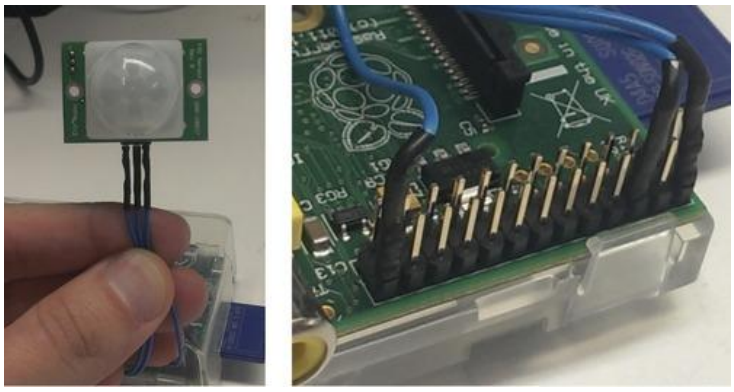
Tavallisesti käyttäjä ohjaa itse laitteita tietokoneella, tabletilla tai älypuhelimella. Kodin automaation toiminta pyritään perustamaan itsenäisesti toimiviin laitteisiin, ja laitekokonaisuuksiin. Tapahtuva toiminta voi olla joko ajastettua, tai toisen laitteen ohjaamaa. Ajastetulla toiminnalla tarkoitetaan että ohjelmoitu funktio tapahtuu tiettyyn kellonaikaan, tai jollain aikavälillä. Tapahtumasta riippuva automaatio taas edellyttää,

että laite saa syötteen anturilta tai toiselta laitteelta tilamuutoksesta. Tällaisia tapahtumia voi olla esimerkiksi liikkeentunnistus ja lämpötilanmuutos. Edellämainittua logiikkaa kutsutaan nimellä IFTTT (If This Then That). Pelkästään näiden tekniikoiden kombinaatioilla voidaan luoda lähes rajattomasti erilaisia älykkäitä ratkaisuja.

5 IOT-LAITEALUSTAT

IoT-alusta on hankalasti rajattava käsite, sillä sitä varten ei ole luotu mitään tietynlaista standardia. Sillä tarkoitetaan kuitenkin laitteistoa tai pohjaa jolla voidaan yhdistää älylaitteet toimimaan yhdeksi kokonaisuudeksi. IoT-alustan tarkoitus on saada laitteiden ja sensoreiden keräämä tieto hyödynnettyä ja tallennettua niin, että sen on käyttökelpoista kaikkien yhdistettyjen laitteiden välillä. IoT-alustan tehtävä on yhdistää käyttäjä, tietojärjestelmä ja laitteet toisiinsa. Alusta integroi, prosessoi ja esittää tiedon ihmiselle ymmärrettävässä muodossa. Tietoliikenne on siis molemminsuuntaista laitteiden ja alustan välillä. Kotikäyttöön IoT-alustan perustaminen ei itsessään ole kallista, sillä hinnat alkavat muutamista kymmenistä euroista ylöspäin, aina hintavampien 100-200 euron hintaluokan laitteisiin asti. (Räisänen 2016)

Kuvassa 1 on esitetty kehitysalustan toimintaa, joka perustuu siihen, että alustaan liitetään kaikki käyttäjän haluamat laitteet tai sensorit sen vapaaseen elektroniikkapiiriin. Kytkentöjen toimintaa muokataan IoT-alustan hallintaan tarkoitetulla ohjelmalla. Tavallisesti konfiguraatio tehdään tietokoneella, mutta muitakin menetelmiä on mahdollista käyttää, kuten kosketusnäyttölaajennuksen kautta suoritettavaa konfiguraatiota.



Kuva 1. Raspberry Pi-alustaan kytkettynä PIR (passiivi infrapuna-anturi)

Laitepohjaisen kokonaisuuden voidaan ajatella olevan koottu kahdesta osasta: palvelinlaitteesta, ja asiakaslaitteesta. Asiakaslaite koostuu alustasta ja siihen liitetyistä laitteista ja sensoreista. Palvelinlaite taas sisältää rajapinnan hallintaan, joka on useimmiten web-pohjainen. Käyttöliittymän kautta käyttäjä hallitsee laitteita ja näkee niiden lähettämän informaation. Käyttötiedot tallentuvat käyttöliittymässä esimerkiksi tekstitiedostoon ohjelmointikielen muodossa. IoT-alusta käy säännöllisesti lukemassa tallennettua tiedostoa, ja kun tiedostoon tulee muutos, välitetään komento asiakaslaitteelle joka suorittaa käskyn laitteessa. (DIYhacking 2014)

5.1 Raspberry Pi

Raspberry Pi on hieman luottokorttia suurempi, yhden piirilevyn tietokone. Raspberry on soveltuva IoT-kehitysalustaksi 40-pinnisen GPIO (General purpose I/O) –piirinsä vuoksi. Tällä hetkellä Raspberry Pi:stä on tehty kolme eri sukupolven mallia, sekä kaksi Raspberry Pi Zero-mallia. Uusin kolmannen sukupolven Pi maksaa noin 35 dollaria, eli sillä voi edullisesti aloittaa IoT-harrastuksen. Laite on varustettu 64-bittisellä, 1.2 gigahertzin neliydinprosessorilla. Käyttömuistia on yhteensä 1 gigatavu. Langattomia yhteystapoja Raspberryssä on WLAN, jolla voidaan muodostaa yhteys verkkoon. Lisäksi sisäänrakennettuna on BTLE (Bluetooth Low Energy)-piiri, jonka avulla voidaan muodostaa Bluetooth-yhteyksiä. Laitteessa ei tule mukana hiirtä, eikä näppäimistöä, joten ne tulee hankkia erikseen. Tällä hetkellä Raspberry Pi on suosituin IoT-kehitysalusta, sen monipuolisten ominaisuuksien sekä edullisen hinnan vuoksi. (RaspberryPi 2017)

Raspberry Pi:n liitännät

- HDMI-portti ulkoisen näytön liittämistä varten
- CSI kameraliitäntä Raspberry Pi kameralaajennukselle
- DSI näyttöliitäntä Raspberry Pi kosketusnäyttölaajennukselle
- mikroSD-portti käyttöliittymää ja tallennettavaa dataa varten
- 4 kappaletta USB 2.0 portteja
- mikro USB-liitäntä, jonka kautta Raspberry saa käyttövirtansa
- 40-pinninen GPIO-liitäntä ulkoisia laitteita varten
- 3,5mm audioliitäntä

Käyttöliittymänä toimii Raspberryn oma Linux-pohjainen versio Raspbian. Raspberry voidaan myös asentaa perinteisellä Linux-käyttöjärjestelmällä toimivaksi, ja se on myös täysin yhteensopiva Android-käyttöliittymän kanssa. Raspberryn vahvuutena on sen mikroSD-korttipaikka. Laitteen käytössä oleva käyttöjärjestelmä asennetaan muistikortille, ja käyttöjärjestelmää voidaan vaihtaa asentamalla toinen muistikortti paikalleen.

5.2 Arduino

Arduino on avoimen lähdekoodin kehitysalusta, ja mikrokontrolleri. Sille komentoketjuja antamalla voidaan siis saada se tekemään tehtäviä, kuten käynnistämään ja ohjaamaan muita laitteita. Se luotiin alkujaan IT-opiskelijoille prototyyppien testaustarkoitukseen. Arduinon hallintaan tarkoitettu ohjelma (Arduino Software) on avoimen lähdekoodin sovellus, joka toimii Windows, Mac, sekä Linux käyttöjärjestelmillä. Arduinosta on valmistettu 15 erilaista mallia, sekä useita epävirallisia variaatioita. Laitteet eroavat toisistaan liitäntäpinnien, sekä keskusmuistin määrässä. (Arduinon www-sivut 2018)

5.3 Intel Galileo

Intel Galileo on Intelin kehittämä Arduino-sertifioitu kehitysalusta, jossa on Intelin 400 megahertzin 32 bittinen suoritin. Galileo on yksipiirilevyinen ratkaisu, johon voidaan liittää laajennuksia. Galileosta on kaksi eri sukupolven mallia, joista tällä hetkellä uusin on Intel Galileo Gen 2. Tämä kehitysalusta soveltuu hyvin sensorien käyttöön sekä valvontaan, koska Galileossa on reaaliaikainen kello. Galileo on myös taaksepäin yhteensopiva aiempien Arduino-laitteiden kanssa. Alusta on oletuksena Linux-pohjainen, mutta on yhteensopiva Windows-, Linux- ja Mac-laitteiden kanssa. Galileo tukee PoE-teknologiaa (Power over Ethernet). Tämä tarkoittaa sitä, että se pystytään konfiguroimaan niin, ettei erillistä virtalähdettä tarvita, vaan käyttövirta saadaan ethernet-verkon kautta laitteelle. Yhtenä negatiivisena ominaisuutena on, että kun alusta sammutetaan, katoaa sen hetkinen data kokonaan. Tämä tilanne pystytään korjaamaan lisäämällä mikroSD-kortti alustaan, jolloin aiempi prosessi voidaan palauttaa muistikortilta. (Reese)

Intel Galileo Gen2 liitännät:

- 14-pinninen digitaalinen I/O
- SPI-liitäntä (tukee aikaisempaa Arduino-teknologiaa)
- analogiset sisääntuloliitännät A0-A5
- SDA ja SCL-liitäntä
- PWM-liitäntä (kahdeksan pinniä, pulssin leveysohjaus)
- 5V virtaliitäntä
- ethernet-liitäntä
- mikroSD-korttipaikka

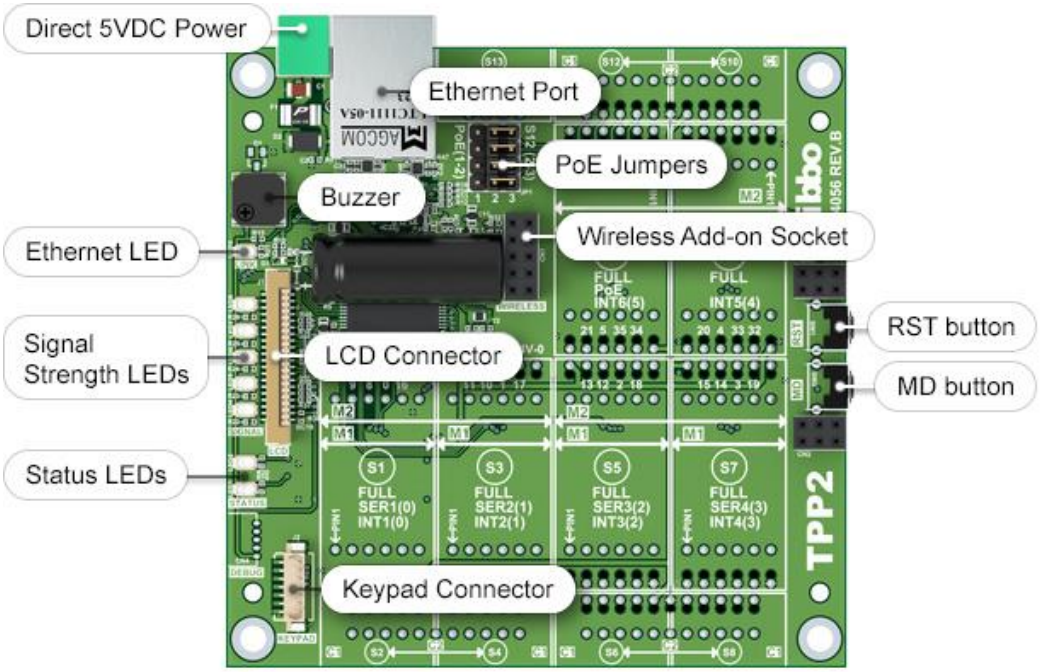
5.4 Tibbo Systems

Taiwanlainen yritys Tibbo Technology Inc. on kehittänyt automaatio- ja IoT-alustan, joka tunnetaan nimellä Tibbo Project System. Laite sisältää mikroprosessorin, ohjelmoitavan piirin sekä I/O-piirin liitettäviä laitteita varten. Laitteen ohjelmointi suoritetaan siihen tarkoitetulla Tibbo IDE-sovelluksella. Ohjelmointikielenä käytetään valmistajan omaa Tibbo Basic-, tai Tibbo C-ohjelmointikieltä. Laitteen vahvuus on sen irroitettavat ja vaihdettavat moduulit, joita on saatavilla kattava määrä eri tarkoituksiin. Erilaisia moduuleita ovat esimerkiksi WiFi-moduuli, lisäosia varten luodut liitäntämoduulit sekä virtamoduulit. Kehitysalustaan on saatavilla valmistajan oma näyttö- ja kosketuspaneeli, joka helpottaa sen hallintaa. Laitteessa on myös PoE-liitäntä (Power over Ethernet). Tibbo soveltuu myös teollisuuden IoT-ratkaisuihin sen hyvän muunneltavuuden vuoksi. (Tibbon www-sivut 2018)

Tibbo Project Gen2 liitännät:

- Ethernet-verkkoliitäntä
- PoE-liitäntä
- LCD-liitäntä näyttöä varten
- liitäntä näppäimistölle
- 5V virtaliitin

Kuvaa 2 tutkiessa voidaan havaita laitteen toiminnan kannalta tärkeät ominaisuudet, kuten virtaliitäntä, Ethernet-liitäntä, ja laitteen sen hetkisestä toiminnasta kertovat ledvalot. Laitteen hallintaan, ja järjestelmämuutoksiin tarvitaan kuitenkin tietokone, jolla muodostetaan yhteys kehitysalustaan. Liitäntämoduulien paikkoja ei ole merkitty kuvaan.



Kuva 2. Tibbo Project Gen2 alusta. Kuvassa näkyy merkittynä laitteen liitännät, laajennusosien liitäntiä lukuunottamatta.

5.5 Laitealustojen vertailu

Edellä on esitelty muutamia kehitysalustoja, joita voidaan hyödyntää kodin automaation hallintaan tavalla tai toisella. Kehitysalustojen tarjonta ei kuitenkaan rajoitu näihin laiteratkaisuihin, vaan tarjolla on useita muitakin ratkaisuja eri valmistajilta. Tarkoituksena oli esitellä muutamia yleisimmin käytettyjä kehitysalustoja, ja vertailla niiden ominaisuuksia keskenään.

Ratkaisuista Raspberry Pi, Galileo sekä Tibbo ovat teknisiltä ominaisuuksiltaan parhaiten vertailukelpoisia, sillä niiden tehot ja käyttömuistin määrä ovat keskenään melko tasavertaisia. Raspberry Pi:n prosessori, sekä yhden gigabitin käyttömuisti soveltuu kuitenkin parhaiten esimerkiksi median toistoon. Arduinon ratkaisua voidaan kutsua ennemminkin mikrokontrolleriksi kuin kehitysalustaksi, sen melko vaatimattomien ominaisuuksien vuoksi. Mallista riippuen Arduino-alustojen 8-84 MHz prosessorinopeus, sekä maksimissaan 96kb:n käyttömuistin määrä, eivät kykene kovinkaan monimutkaisiin tehtäviin. Muut vertailussa olevat laitteet pystyvät suorittamaan useita

prosesseja samanaikaisesti. Arduino sopiikin vain yksinkertaisiin käyttötarkoituksiin, kuten esimerkiksi autotallin oven automatisointiin, tai vaikka lämpötilan mittaukseen.

Intel Galileon positiivisena puolena on, että se on yhteensopiva aiempien Arduino-ratkaisujen kanssa, ja niistä voidaan rakentaa yhdessä toimivia kokonaisuuksia. Tibbon kehitysalusta on vaihdettavien moduuliensa ansiosta hyvin kustomoitavissa kunkin käyttäjän omaan tarkoitukseen. Käytännössä se tarkoittaa kuitenkin sitä, että moduulit tulee ostaa erikseen, joka lisää Tibbon hankintahintaa. Tibbon alusta saattaa muutenkin ominaisuuksiensa puolesta olla enemmän soveltuva teollisuuden käyttötarkoituksiin. Yksi Raspberry Pi:n ominaisuuksista erottuu merkittävästi joukosta, sillä se on ainoa ratkaisu, jonka piirilevyn liitännöistä löytyy HDMI-liitäntä ulkoista näyttöä varten. Myös saatavuuden ja hintansa puolesta Raspberry Pi on edellä muita valmistajia.

6 PILVIPOHJAISET IOT-ALUSTAT

Pilvipohjaisten IoT-alustojen tarjonta on kasvusuuntainen, aivan kuten laitepohjaisten IoT-alustojenkin tarjonta. Niiden toiminta perustuu pitkälti pilvipalveluiden PaaS-palvelumalliin (Platform as a Service). Pilvipohjaisissa ratkaisuissa laitteet yhdistyvät verkkoon hubin, tai yhdyskäytävän (gateway) kautta. Mahdollista on myös että IoT-laite muodostaa suoraan yhteyden verkkoon ilman erillistä yhdyskäytävää. Laitteiden lähettämä data välittyy pilvialustalle, jossa se prosessoidaan ja yhdistetään muiden laitteiden datan kanssa. Pilvialusta siis kerää tietoja fyysisiltä laitteilta (klientit) ja yhdistää ne suuremmaksi datakokonaisuudeksi, jota voidaan hyödyntää laitteiden kesken. (James 2016)

Pilvipohjaisen IoT-arkkitehtuurin muodostavat kolme tekijää:

- laitteet (klientit)
- yhdyskäytävä (gateway)
- pilvipalvelu

Pilvialustalla on keskitetty tietokanta johon jokainen laite erikseen rekisteröidään. Laitteiden rekisteröinti on tarpeellista koska pilvipalvelu luo jokaiselle laitteelle oman SSL/TLS-sertifikaatin ja käyttöavaimen, jonka avulla tiedonvälitys on mahdollista. Näitä suojaustapoja käytetään pilvipalvelun ja laitteen välillä autentikointiin ja tiedonsuojaukseen. (Falck 2017)

IoT pilvialustaa ei tule kuitenkaan sekoittaa pilvilaskentaan, vaikka Internet Of Thingsin toimintaan liittyy vahvasti pilvipalvelut. Pilvialustoihin nimittäin liittyy enemmän ominaisuuksia, joista voidaan mainita laitteiden hallinta ja analyyttiset toimintamallit. Esimerkiksi osa autonvalmistajista tukee IoT-teknologiaa siten, että kuluttaja pystyy liittämään oman ajoneuvonsa järjestelmän pilvipohjaiseen IoT-alustaan. Tämän avulla käyttäjä saa ilmoituksen mahdollisista tulevista huolloista, varaosatarpeista, tai vaikkapa lähestyvästä katsastustarpeesta. Työssä esitellyt pilvipohjaiset ratkaisut ovat saatavilla niin yrityksille, kuin kuluttajillekkin.

6.1 AWS

AWS eli Amazon Web Services on Amazonin perustama pilvipohjainen IoT-alusta. AWS IoT on täysin hallinnoitu palvelu, eikä palvelun käyttäjän tarvitse huolehtia serverin määrityksistä tai järjestelmäpäivityksistä. Palvelu näkyy käyttäjälle ohjelmointirajapintana, josta hallitaan käyttäjän liittämiä laitteita. Viestintä tapahtuu MQTT-protokollaa käyttäen. Amazon tarjoaa käyttäjälle Device SDK (Software Development Kit) sovellustyökalun jolla saadaan fyysinen laitteisto toimimaan pilvipalvelun kanssa. Sovellustyökalu sisältää avoimen lähdekoodin lähdekirjaston, joka auttaa konfiguroinnin kanssa. AWS:n käyttö on hyvin edullista, sillä maksu peritään vain toteutuneen käytön mukaisesti. Miljoonasta toteutuneesta palveluviestistä käyttömaksu on viisi dollaria. (Falck 2017)

6.2 Microsoft Azure IoT Hub

Azuren palvelualusta tarjoaa sen käyttäjälle tietoturvallisen ratkaisun yhdistää fyysiset laitteet pilveen, sekä mahdollistaa kaksisuuntaisen kommunikoinnin laitteiden ja pilvialustan välillä. Azure IoT Hub sisältää valinnaisen tallennustilan laitedatalle, sekä tukee IoT-laitteiden kehitystä Azure palvelurajapinnan avulla. Palvelu on yhteensopiva Windows-, Linux-, iOS- ja Android-käyttöjärjestelmien kanssa. Azure IoT Hub:in hyödyllisenä ominaisuutena on sen yhteensopivuus muiden Azure-palveluiden kanssa kuten datamassojen analysointi (Big Data) ja koneoppiminen (Machine Learning).

Palvelun käyttöönottoa on helpotettu Azure Suite ohjelmakirjastolla, jossa on koottuna valmiita IoT-pohjaratkaisuja mitä voidaan kustomoida omiin tarpeisiin sopivaksi. Tiedonsiirtoon käytetään HTTP-, AMQP- ja MQTT-protokollia. Laitteiden yhdistäminen jotka eivät tue edellämainittuja protokollia, on mahdollistettu avoimen lähdekoodin yhdyskäytävän avulla. Yhteys voidaan siis saada suoraan laitteen ja pilvipalvelun välillä, tai vaihtoehtoisesti yhdyskäytävän (gateway) välityksellä. Palvelun käyttö on ilmaista 8000 viestiin/päivässä asti. (Bloch 2016)

6.3 Google Cloud Platform

Google Cloud Platform on Goolgen hallinnoima pilvialusta, joka koostuu useista Googlen tarjoamista palveluista. Sen avulla voidaan kerätä, prosessoida ja analysoida IoT-laitteiden dataa reaaliajassa ja kustannustehokkaasti. Google tekee IoT-kehitystyötä laitevalmistajien kanssa, joista merkittävimpiä nimiä ovat Intel, Cisco sekä Sierra Wireless. Tämä parantaa yhteensopivuutta “raudan” ja ohjelmistojen osalta. (Googlen www-sivut 2017)

Google Cloud Platform on sen käyttäjien osalta serverivapaa, eli käyttäjän ei tarvitse rakentaa toimivaa infrastruktuuria. Laitteet yhdistetään suoraan Googlen IoT Core-palveluun käyttäen HTTP- tai MQTT-protokollaa. Käyttäjän ei tarvitse osallistua ylläpitoon, ja käyttömaksu perustuu kuukausittaiseen datansiirtomäärään. Kuukausittain 250 megabittiin asti käyttö on ilmaista, joka riittää harrastelijakäyttöön hyvin.

6.4 Pilvialustojen vertailu

Tässä työssä esiteltyjen pilvipohjaisten IoT-alustojen lisäksi saatavilla on useita muita ratkaisuja eri yrityksiltä. Googlen, Azuren ja Amazonin alustat ovat eniten käytettyjä kuluttajatasolla. Niiden käyttöönotto on tehty yksinkertaiseksi, sekä käyttöä varten löytyy palveluntarjoajan sivulta kattavasti ohjeita. Kaikkilla vertailussa olevilla alustoilla on oma sovelluskehitys kirjastonsa (SDK), josta löytyy valmiita malliratkaisuja kustomoitavaksi.

Yhteistä näillä kolmella on että niiden perusominaisuuksien käyttö on ilmaista, tai lähes ilmaista. Palvelut ovat hinnoiteltu joko toteutuneen käytön mukaisesti tai porrastetusti. Tavallisesti ilmaisversion käyttö on rajoitettu datankäytön osalta, ja esimerkiksi palvelun tallennustilan käytöstä pitää maksaa erikseen. Toisaalta yksittäisen kotitalouden automatisoinnin kannalta lisäominaisuudet, kuten datan analysointi tai suurien datamäärien varastointi ei ole pakollista. Palvelua voidaan käyttää pelkistetysti vain laitteiden ohjaukseen, ja muut ominaisuudet ovat valinnanvaraisia.

7 YHTEYSTYYPIT

Toimivan IoT-struktuurin edellytys on laitteiden välinen kommunikointi. Siten laitteet pystyvät viestimään toisilleen, ja lähettämään dataa sovelluksien ja palvelujen välillä. Verkostoituminen tapahtuu käyttäen yhtä tai useampaa tiedonsiirtomenetelmää. Tiedonsiirto voi tapahtua langattomasti tai kiinteän verkkoyhteyden avulla. Langallinen yhteys on luonnollisesti nopein ja luotettavin yhteystapa, mutta sen käyttö ei ole kaikissa tapauksissa mahdollista. Langattomat tiedonsiirtotekniikat ovat yleistyneet, ja useita sen tarjoamia standardeja voidaan hyödyntää älylaitteiden yhteyksien muodostamiseen.

7.1 WiFi

Langattoman lähiverkon teknologiaa kutsutaan nimellä WiFi, tai WLAN. WiFi perustuu IEEE 802.11–standardiin. WiFi-teknologian avulla voidaan muodostaa langaton lähiverkko, ja liittää siihen laitteita jossa on WiFi-vastaanotin. Langaton lähiverkko luodaan WLAN-tukiasemalla, joka lähettää radioaaltojen avulla signaalin vastaanottavalle laitteelle. Signaalin kantavuus on noin 20-50 metriä, ja ulkotiloissa noin 100 metriä. Signaalin vahvuuden heikentyessä, myös tiedonsiirron nopeus heikkenee. Useammalla WLAN-tukiasemalla, tai verkon toistimella kantavuutta voidaan laajentaa. Taajuusalueena käytetään yleisesti 2.4GHz ja 5GHz taajuuksia. Näiden erona 5GHz taajuus on tiedonsiirrollisesti nopeampi, ja 2.4GHz taajuudella kantomatka on pidempi. (CCM 2017)

7.2 Bluetooth

Bluetooth on langattoman tiedonsiirron-standardi, jonka kehitti Ericsson Mobile yrityksen teknologiajohtaja Nils Rydbeck, vuonna 1989. Bluetooth on tarkoitettu lähietäisyydellä toisistaan olevien elektronisten laitteiden langattomaan tiedonsiirtoon. Sen toiminta tapahtuu 2.4GHz radiotaajuudella, ja tiedonsiirtonopeus on 1Mbps luokkaa. Bluetooth-laitteiden välinen yhteys vaatii laitteiden “parittamisen” ennenkuin ne kykenevät siirtämään dataa keskenään. Laitepari hyväksytään molemmissa laitteissa esimerkiksi pin-koodilla. Parituksen jälkeen laitteet muistavat toisensa, ja pystyvät toistensa kantama-alueella ollessaan lähettämään dataa. Signaalin kantavuus on välillä 10-100 metriä, riippuen laitteiden Bluetooth-versiosta. (Sparkfun 2017)

Bluetoothin versio 4.0 sisältää ominaisuuden BLE (Bluetooth Low Energy) joka kuluttaa vähemmän virtaa kuin tavanomainen Bluetooth. BLE on kehitetty juuri IoT-tarkoitukseen, koska se pidentää akku- tai paristokäyttöisten laitteiden toiminta-aikaa merkittävästi. Pienempi virrankulutus perustuu laitteiden tiedonsiirron minimoimiseen. Dataa lähetetään vain silloin kun on tarve, ja muutoin laite on virransäästötilassa. BLE-teknologialle ominaista on että siirrettävät datamäärät ovat kooltaan pieniä. (Sparkfun 2017)

Bluetooth 5.0 version myötä kantama laitteiden välillä saatiin moninkertaistettua, noin 40-400metriin. Tiedonsiirtonopeus on kaksinkertainen verrattuna aiempaan versioon, joka tarkoittaa 2Mbps nopeutta. Uutena ominaisuutena myös useamman laitteen samanaikainen yhteys, esimerkkinä kaksi medialaitetta voi toistaa samaa sisältöä yhdestä puhelimesta. (Tucker 2017)

7.3 ZigBee

ZigBee Alliancen kehittämä langaton lyhyen kantaman likiverkko (WPAN), joka on kehitelty erityisesti IoT-yhteyksiä ajatellen. ZigBee toimii 2.4GHz:n radiotaajuudella. Lähetysnopeus on 250kbps, joka on riittää hyvin sensorien ja ohjainten datan siirtoon. Sen toimintasäde on 10-100 metriä, sekä komponentit ovat edullisempia kuin WiFi- tai Bluetooth-laitteiden vastaavat komponentit. Vaikka ZigBee-teknologia vastaa paljon WiFi-teknologiaa, ei sen tarkoitus ole kilpailla sitä vastaan, vaan tarkoituksena on saada mahdollisimman pienellä viirrankulutuksella toimiva tietoliikenneverkko. (Agarwal)

7.4 NFC

NFC (Near-field Communication) on RFID-tunnisteisiin pohjautuva kommunikointiprotokolla elektronisten laitteiden välillä. NFC:n toiminta perustuu sähkömagneettiseen induktioon laitteiden välillä, joka tapahtuu 13.56MHz:n taajuudella. Tiedonsiirtonopeudet vaihtelevat 106-424 kilobittiin sekunnissa. Se mahdollistaa toisistaan 4-5 senttimetrin etäisyydellä olevien laitteiden “kättelyn” ja tiedonvaihdon. Autentikointi tapahtuu asettamalla laitteet toistensa lähelle, joten luonnollisesti sen käyttö on tietoturvallisuuden näkökulmasta turvallista. (Poole)

NFC menetelmää voidaan käyttää laitteiden välillä, joissa on NFC-siru, ja sen lisäksi on mahdollista käyttää NFC-tageja. Tagit ovat passiivisia elektroniikkapiirejä, jotka saavat virtansa NFC-laitteesta, jolla tagit luetaan. Näin ollen ne eivät tarvitse erillistä virtalähdettä. Tagit voivat sisältää dataa, kuten verkko-osoitteita, tekstirivejä tai yhteystietoja. Niiden avulla voidaan myös suorittaa toimintoja esimerkiksi älypuhelimessa, kun puhelin viedään NFC-tagin lähelle. (Triggs 2017)

Tuttu esimerkki NFC:n toiminnasta on lähimaksusiru, joka löytyy useimmista uusista pankkikorteista. Lähimaksuominaisuus voidaan myös toteuttaa puhelimen NFC-piirin avulla. Lähimaksun avulla käyttäjän ei tarvitse maksutapahtuman yhteydessä näppäillä kortin pin-koodia, vaan maksu hyväksytään asettamalla maksukortti tai puhelin maksupäätteen lukuetäisyydelle.

7.5 Z-Wave

Z-Wave on ZenSys:n kehittämä matalan virrankulutuksen langaton protokolla, joka on suunniteltu ensisijaisesti kodin automaation käyttötarkoituksiin. Liikennöinti tapahtuu 900 MHz taajuudella, ja verkon rakenne on mesh-pohjainen. Kantavuus esteettömässä tilassa on noin 100 metriä. Verkko koostuu ohjaimesta tai ohjaimista, ja siihen liitetyistä moduuleista (node). Ohjaimen tehtävä on muodostaa yhteys internetiin, ja luoda tiedonsiirtoreitit moduulien välillä. Yksittäinen laite pystyy lähettämään sekä vastaanottamaan käskyjä. Jokainen Z-Wave laite pystyy myös valvomaan muiden laitteiden tilaa ja raportoimaan tiedon ohjaimelle. Toisin sanottuna siis yksittäinen laite toimii verkon toistimena. Jos yksittäinen moduuli ei ole verkon kantoalueella, mutta on toisen moduulin kantoalueella, saadaan yhteys ohjaimelle toisen moduulin välityksellä. Mitä useampi laite verkkoon on yhdistettynä, sitä tehokaammaksi sen toiminta muuttuu. Yhteen verkkoon voi olla liitettynä yhteensä 232 moduulia, sekä verkkoja voidaan yhdistää toisiinsa. (Sciacca 2013)

Z-Waven etuna on vähäinen virrankulutus. Sen virrankulutus on WiFi-teknologiaa pienempi, jolloin patteri- ja akkukäyttöisten laitteiden huoltoväli voi olla useita vuosia. Tämä ominaisuus on yksi avaintekijöistä langattoman kodin automaation suunnittelua ajatellen.

7.6 Matkapuhelinverkko

Matkapuhelinverkkoa voidaan hyödyntää IoT-laitteiden tiedonsiirrossa. 3G- ja 4G-yhteyksillä tiedonsiirtonopeudet riittävät suurempienkin datamäärien siirtoon. Ongelmakohtana tässä on korkea virrankulutus ja operaattorien dataliittymien korkeat hinnat. Tyypillisten mobiililiittymien tiedonsiirtonopeus on IoT-laitteiden kannalta ylimitoitettu, koska laitteiden lähettämä anturi- tai mittausdata on keskimäärin kooltaan vain muutamia kymmeniä bittejä. (Hwang 2016)

Tähän tilanteeseen on kehitelty maailmanlaajuisesti uusia standardeja joiden ominaisuudet ovat mobiiliverkkojen ominaisuuksia vastaavia, kuten LoRaWAN ja ranskalaisen Sigfoxin käyttämä UNB (Ultra Narrow Band). Nämä tiedonsiirtotekniikat ovat mobiiliverkkoteknologiaa kevyempiä, ja kantavuudeltaan jopa 50-100 kilometriä. Ominaisuuksiin kuuluu pienehköt datansiirtopaketit ja hyvin pieni virrankulutus. (Hwang 2016)

8 TIETOTURVA

Kodin laitteiden yhdistäminen internetiin kuulostaa lupaavalta idealta, mutta asioihin tulee kiinnittää turvallisuusnäkökulmasta erityistä huomiota. Yhteistä älylaitteilla on se, että ne kaikki ovat yhteydessä verkkoon, ja ilman verkkoyhteyttä niiden toiminta yhdessä ei ole mahdollista. IoT-verkkoliikenne kulkee yleisesti julkisen internetin välityksellä käyttäen TCP/IP tai UDP- verkkoja.

Kodin IoT-laitteita hankkiessa kuluttajalla ei todennäköisesti ole ensimmäisenä asiana mielessä tietoturva. Tietoturva-asioista ei välttämättä myyjäliikkeessä kerrota, tai edes valmistajan puolesta riittävää informaatiota ei ole saatavilla. Osa kuluttajista ostaa tuotteensa tunnetuilta valmistajilta, koska luotetaan niiden tietoturvallisuuspuolen olevan kunnossa. Tämä oletus kuitenkaan harvoin pitää paikkaansa. Tietoturvapuoli saattaa jäädä kuluttajan omille harteille. (Nortonin www-sivut 2017)

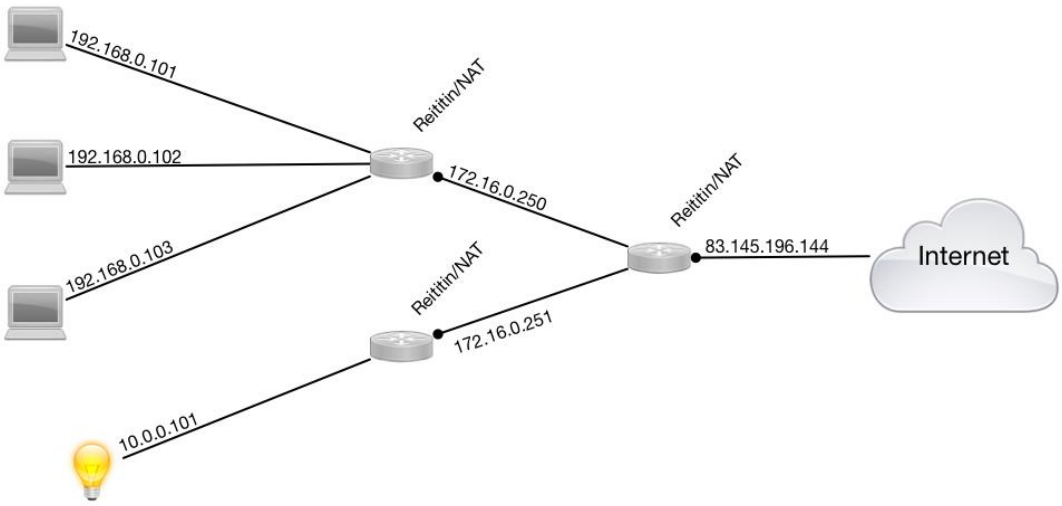
Accenturen tekemän IoT-tutkimuksen mukaan älylaitteiden käyttäjistä 18% on päättänyt palauttaa laitteen ostopaikkaan, ja lopettaa älylaitteiden, tai niihin liittyvien palveluiden käytön kokonaan kunnes uskovat sen olevan turvallista. 24% kyselyyn osallistujista ovat kiinnostuneita teknologiasta, mutta toistaiseksi eivät aio käyttää kyseisiä laitteita tai palveluita. Reilu neljännes käyttäjistä on tietoisia riskeistä, ja aikovat olla tulevaisuudessa varovaisempia teknologian käyttöön liittyvissä asioissa. Vain 21% kannanottajista on sitä mieltä että IoT-laitteiden käyttö on turvallista, ja pitävät uhkia kuten hakkerointia epätodennäköisenä vaihtoehtona. (Accenture 2014)

Edellämainitusta tutkimuksesta voimme päätellä, että kuluttajat eivät ole vielä täysin luottavaisia älylaitteiden toimintaan. Kuluttajien epäröinti teknologiaa kohtaan on osittain aiheellista. Mediassa uutisoidaan toistuvasti yrityksiin, ja organisaatioihin kohdistuneista tietomurroista. Usein vääriin käsiin saatu data sisältää käyttäjätunnuksia, salasanoja, henkilötunnuksia, tai luottokorttitietoja. IoT-laitteiden tietoturva ei ole tässä asiassa poikkeus, sillä ne ovat yhtävertaisesti haavoittuvaisia tietovarkauksille. Tietomurrot ovat näkymätön uhka, johon ei osata suhtautua oikealla tavalla. Älyratkaisuja tarjoavien yritysten tulisi paneutua tietoturvallisuuteen paremmin, koska se on yksi edellytys käyttäjätyytyväisyydelle, ja asiakaskunnan säilymiselle.

8.1 Kotiverkon tietoturva

Kodin internet-verkon oikeaoppisella suojauksella voidaan tehokkaimmin vaikuttaa IoT-laitteiden tietoturvaan. Reitittimen tai langattoman tukiaseman palomuuri tulisi olla käytössä, sekä hallintaan tarvittavat käyttäjätunnus ja salasana kannattaa vaihtaa heti kotiverkkoa käyttöönottaessa. Yksinkertaisin tapa väärinkäyttäjälle päästä käsiksi verkkoon, on kokeilla tukiaseman tehtaalla määritettyjä oletustunnuksia. Jos kotona on käytössä langaton verkko, tulisi siihen liittyminen suojata myös salasanalla. WPA- tai WPA2-suojausprotokollaa käytettäessä kaikki verkon käyttäjät autentikoidaan salasanaa käyttäen, ja tukiasema pystyy tunnistamaan kunkin käyttäjän läsnäolon. WPA-suojaus sisältää TKIP (Temporal Key Integrity Protocol) tai AES (Advanced Encryption Standard) kryptauksen, eli tiedonsiirron salauksen.

Jos kodin IoT-laitteet halutaan hajauttaa kotiverkon muista laitteista, voidaan kotiverkko jakaa osiin. Jakaminen voidaan suorittaa joko loogistesti tai fyysisesti. Loogisella verkon jakamisella tarkoitetaan verkon osittamista virtuaalisesti VLAN-tekniikan avulla (Virtual LAN). Tähän toteutukseen vaaditaan reititin, joka tukee VLAN:ia. Virtuaalisesti jaetun verkon ylläpitäminen saattaa olla kuitenkin työlästä, kun esimerkiksi laitteita lisätään kotiverkkoon. (Järvinen 2016)



Kuva 3 Tietoturvallinen fyysisesti jaettu lähiverkko, jossa IoT-laitteet ovat oman reitittimensä takana.

Fyysisesti jaetulla verkolla tarkoitetaan, että verkko jaetaan reitittimien avulla osiin. Useamman reitittimen avulla voidaan osittaa lähiverkko useampaan verkkoon, jotka eivät ole toisiinsa suoraan yhteydessä. Kuvan 3 verkkoratkaisussa juurireititin muodostaa yhteyden julkiseen internetiin, ja kaksi muuta reititintä jakavat lähiverkon erillisiin osiin. Reitittimien tehtävänä on tässä estää suora kommunikointi IoT-verkon ja muun kotiverkon välillä, sekä suorittaa osoitteenmuunnos NAT-palvelun (Network Address Translation) avulla. Reitittimien tekemän osoitteenmuunnoksen ansiosta kotiverkon laitteiden IP-osoitteet ovat piilotettuina, eikä niihin voida kohdistaa hyökkäyksiä tai porttiskannauksia IoT-laitteiden kautta. (Järvinen 2016)

Tehostettuun kotiverkon valvontaan on hiljattain kehitelty uusia ratkaisuja, kuten älykkäät kodin palomuurit. Älykkäällä palomuurilla tarkoitaan laitepohjaista palomuuria joka liitetään kotiverkkoon. Älykäs palomuuri valvoo kotiverkon liikennettä, ja ilmoittaa, sekä estää epäilyttävältä vaikuttavat toimenpiteet. Tämä laite-kategoria on vain muutamia vuosia vanha, joten voidaan sanoa että sen osalta ollaan vielä kehityksen alkuvaiheessa. Älykkäitä palomuuriratkaisuja ovat esimerkiksi Norton Core, Cujo sekä Bitdefender Box. Laitteiden hinta lähtee noin 200 dollarista, joka sisältää itse laite-palomuurin, sekä rajoitetun määrän käyttöaikaa. (Colburn 2017)

8.2 Laitteiden tietoturva

IoT-laitteet itsessään ovat kokonaisuutta tarkastellessa suurin riskitekijä haavoittuvuuksille. Tekemällä muutamia asioita oikein, voidaan riskejä kuitenkin minimoida. Esimmäisenä tulisi miettiä, onko jokaisen laitteen kytkeminen internetiin todella tarpeellista, ja että saavutetaanko sillä mitään todellista hyötyä. Vaikka laitteen tekniset ominaisuudet mahdollistavatkin verkkoon liittymisen, on syytä miettiä voiko siitä seurata riskejä kotiverkon turvallisuuteen liittyen. Osa älykkäiden laitteiden ominaisuuksista on käytettävissä myös ilman verkkoyhteyttä.

Tyypillisesti laitteiden määritysvaiheessa luodaan käyttäjätunnus, sekä salasana jonka avulla niitä päästään käyttämään. Tehtaalla laitteeseen määritetyt tunnukset ja salasanat tulee vaihtaa riittävän monimutkaisiksi, jotta niitä on vaikeampi murtaa. Vahvan salasanan ominaisuuksiin kuuluu riittävä pituus merkkejä, 8-merkkinen salasana on huomattavasti vaikeampi murtaa kuin 4-merkkinen salasana. Vahva salasana sisältää sekä pieniä, että isoja kirjaimia sekä numeroita. Varminta on luoda jokaisen IoT-laitteen käyttöön eri salasana, jotta kaikki laitteet eivät olisi vaarassa yksittäisen laitteen joutuessa tietomurron kohteeksi. Salasanojen vaihto säännöllisesti olisi suositeltavaa. (Drolet 2016)

Laitteiden ohjelmistoversiot tulisi pitää ajantasalla, sillä vanha ohjelmistoversio saattaa sisältää tietoturva-aukkoja tai muita haavoittuvuuksia, joita hyökkääjä voi käyttää hyödykseen. Uusimpaan ohjelmistoversioon on yleensä tehty virheenkorjauksia, sekä paikattu siihen mennessä havaitut tietoturva-aukot, joten ohjelmiston pitäminen ajantasalla on tärkeä osa turvallisuutta. Kaikkiin älylaitteisiin ei ole saatavilla tietoturvaohjelmistoa, mutta tärkeimpiin laitteisiin on. Tietokoneet, tabletit ja älypuhelimet ovat kasvavassa määrin sidoksissa kodin automaation hallintaan. Tämänkaltaiset laitteet, joilla ohjataan IoT-laitteita, tulisi suojata tietoturvaohjelmistolla. Älypuhelin jolla voidaan hallita kodin automaatiota, tulisi suojata vähintäänkin näyttölukolla, siltä varalta että laite joutuu vääriin käsiin tai varastetaan.

8.3 Pilvipalveluiden tietoturva

Pilvipohjaiset IoT-palvelut perustuvat pilvipalveluiden PaaS-toimintamalliin. Tällä tarkoitetaan, että käyttäjälle tarjotaan alusta sovellusten hallintaa ja kehittämistä varten. Laiteresurssit eivät ole siis käyttäjän hallittavissa, vaan ovat ostettu palveluna palveluntarjoajalta. Palveluntarjoajaa valitessa tulisi arvioida sen toimintaa, sekä selvittää palvelun käyttöön liittyvät ehdot. Suurin osa palveluntarjoajista ilmoittaa käyttöehdoissa mitkä asiat ovat käyttäjän omalla vastuulla ja mitkä eivät. Esimerkiksi datan omistajuuteen liittyvät asiat on oleellista selvittää. Myös mahdollisiin sertifiointeihin on hyvä tutustua. Useimmat pilvipalveluita tarjoavat yritykset pyrkivätkin tekemään omasta toiminnastaan mahdollisimman läpinäkyvää, vaikka kaikkien yksityiskohtien selvittäminen ei olekkaan mahdollista tietoturvallisuuden säilyvyyden vuoksi. (Kyberturvallisuuskeskus 2014)

Koska IoT-palveluiden ominaisuuksiin kuuluu laitteiden hallinta mistä tahansa, toiminta palveluntarjoajan ja käyttäjän välillä perustuu luottamukseen. Pilvipalveluiden käytön kannalta oleellisessa asemassa onkin tunnistautuminen, koska se on ainoa tapa palveluntarjoajalle kontrolloida käyttäjän tietoihin pääsyä. Käyttöliittymät joista päästään ylläpitämään järjestelmiä, tulisi suojata vahvalla todennuksella. Vahva todennus perustuu laitteiden autentikointiin, sekä lisäksi salasanaan, tai pin-koodiin jonka vain käyttäjä itse tietää. Useimmat palvelut tukevat myös kaksiosaista tunnistautumista. (Wallenius 2016)

9 POHDINTA

Aiheeseen olen itse tutustunut ensimmäistä kertaa vuonna 2016 keväällä, jolloin harjoittelimme opinnäytetyön kirjoittamista “Opinnäytetyö ja seminaari”-kurssin muodossa. Tällöin tein työn aiheesta IoT, jonka totesin melko nopeasti olevan liian laaja aihealue opinnäytetyön aiheeksi. Päätin kuitenkin palata aiheen pariin, mutta kuluttaja-IoT aiheeseen rajatulla työllä.

Opinnäytetyön tarkoitus oli avata Internet Of Thingsin toimintapoja, ja selvittää mistä osista toimiva ratkaisu voidaan rakentaa kuluttajaa ajatellen. Työssä olen käynyt läpi lähinnä aiheen perusidean, ja millä komponenteilla, sekä palveluilla kuka tahansa pääsee asian tiimoilta alkuun. Sopivan työmäärän rajaaminen oli hankalaa, sillä aiheesta löytyy paljon asiatekstiä, mutta paljon myös sellaista materiaalia, joka ei ei liity varsinaisesti tämän opinnäytetyön aihealueeseen. Osa työn aihepiireistä oli minulle ennestään tuttuja, kuten yhteysmenetelmät, ja niistä olikin helpompi kirjoittaa. Työssä käyttämäni lähteet ovat kaikki internet-lähteitä, sillä aiheesta ei ollut saatavilla kirjoja kuin muutamia, ja niiden hankkiminen olisi ollut haastavaa.

Jälkeenpäin ajateltuna olisin voinut kertoa myös IoT-sovelluksista, joilla varsinainen hallinta ja konfigurointi tapahtuu. Päätin jättää sen osion kuitenkin työn ulkopuolelle, sillä se olisi vaatinut paljon pidempiaikaista perehtymistä, sekä sovellusten itsenäistä testausta. Työssä esittelin pilvipohjaiset palvelut päällisinpuolin, ja olen selvittänyt niiden ominaisuuksia, sekä palveluntarjoajien hinnoitteluja palvelun käyttöön liittyen.

Vaikka valmis opinnäytetyöni onkin vain pintapuolinen katsaus kuluttaja-IoT:n toimintaan, olen saanut itse paljon enemmän informaatiota asiaan liittyen. Uskoisin että valitsemani aihe on niin sanotusti “tulevaisuuden aihe” josta on minulle itselleni hyötyä myöhemmin esimerkiksi työelämässä. Työn aikana sain täysin uuden näkemyksen siitä miten vahvasti IoT on jo nyt käytössä, ja näkyvillä yhteiskunnan toiminnassa. Oma näkemykseni on että tulevina vuosina, ja vuosikymmeninä olemme menossa yhä enemmän siihen suuntaan, että tietokoneet ja laitteet tulevat ohjaamaan päivittäisiä askareita.

LÄHTEET

Accenture. 2014. Igniting Growth In Customer Technology. Viitattu 26.01.2018. https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf#zoom=50

Agarwal Tarun. ZigBee Wireless Technology, Architecture And Applications. Viitattu 16.01.2018. https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/

Arduino. 2017. What is Arduino?. Viitattu 10.1.2018. https://www.arduino.cc/en/guide/introduction

Bloch Olivier. 2016. Developer's introduction to Azure IoT. Viitattu 22.1.2018. https://azure.microsoft.com/en-us/blog/developer-s-introduction-to-azure-iot/

Bogdanov Vik. 2017. Viitattu 9.1.2018. http://iot.intersog.com/blog/iot-platforms-overview-arduino-raspberry-pi-intel-galileo-and-others/

CCM. 2017. Introduction to Wi-Fi (802.11 or WiFi). Viitattu 15.1.2018. http://ccm.net/contents/802-introduction-to-wi-fi-802-11-or-wifi

Colburn Ken. 2017. Smart firewalls protect the Internet of Things – Which are the best? Viitattu 14.02.2018. https://wtop.com/tech/2017/10/smart-firewalls-protect-internet-things-best/

DIYhacking. 2014. Web Based Automation For Your Home With Raspberry Pi!. Viitattu 8.1.2018. https://diyhacking.com/raspberry-pi-home-automation/

Drolet Michelle. 2016. 8 tips to secure those IoT devices. Viitattu 07.02.2018. https://www.csoonline.com/article/3085607/internet-of-things/8-tips-to-secure-those-iot-devices.html

Falck Kenneth. 2017. How Amazon's IoT Platform Controls Things Without Servers. Viitattu 10.1.2018. https://www.nordcloud.com/tech-blog/how-amazons-iot-platform-controls-things-without-servers

Friedemann M. & Floerkemeier C. 2010. Internet Of Things. Viitattu 8.1.2018. http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

Hardik Shan. 2017. Home Automation Using IoT. Viitattu 8.1.2018. https://dzone.com/articles/home-automation-using-iot

Hendricks Drew. 2014. The History of Smart Homes. Viitattu 17.01.2018. http://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm

Hwang Yitaek. 2016. Cellular IoT Explained NB-IoT vs. LTE-M vs. 5G and More. Viitattu 25.01.2018. https://www.leverege.com/blogpost/cellular-iot-explained-nb-iot-vs-lte-m

James Richard. 2016. IoT platform explained in detail. Viitattu 10.1.2018. https://medium.com/@richjam16/iot-platform-explained-in-detail-6f685b6adcb6

Järvinen Antti. 2016. IoT-laitteet turvallisesti lähiverkossa. Viitattu 01.02.2018. http://alupark.fi/blog/2016/03/iot-laitteet-turvallisesti-lahiverkossa/

Knowyourmeme. 2010. Internet Coke Machine. Viitattu 8.1.2018. http://knowyourmeme.com/memes/internet-coke-machine

Kyberturvallisuuskeskus. 2014. Pilvipalveluiden turvallisuus. Viitattu 05.03.2018. https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Maney Kevin. 2014. Kevin Ashton, Father of the Internet of Things & Network Trailblazer. Viitattu 8.1.2018. https://newsroom.cisco.com/feature-content?articleId=1558161

Meola Andrew. 2016. How IoT & smart home automation will change the way we live. Viitattu 8.1.2018. http://nordic.businessinsider.com/internet-of-things-smart-home-automation-2016-8?r=US&IR=T

Nortonin www-sivut. 2017. 4 steps to make your smart home more security smart. Viitattu 26.01.2018. https://us.norton.com/internetsecurity-iot-4-steps-to-make-your-smart-home-more-security-smart.html

Poole Ian. NFC Technology. Viitattu 16.01.2018. http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-technology.php

RaspberryPi. 2017. Viitattu 9.1.2018. https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

Reese Lynnette. A Comparison Of Opensource Hardware: Intel Galileo vs. Raspberry Pi. Viitattu 9.1.2018. https://www.mouser.fi/applications/open-source-hardware-galileo-pi/

Russell Brad. 2018. Cloud Platform trends for the smart home. Viitattu ??.1.2018. http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Cloud-platform-trends-for-the-smart-home

Räisänen Paula. 2016. Internet of Things valmiit alustat testissä pt.1. Viitattu 8.1.2018. https://www.linkedin.com/pulse/internet-things-valmiit-alustat-testiss%C3%A4-pt-1-paula-r%C3%A4is%C3%A4nen

Sciacca John. 2013. Smarten up your dumb house with Z-Wave automation. Viitattu 24.01.2018. https://www.digitaltrends.com/home/smarten-dumb-house-z-wave-automation/

Sparkfun. 2017. Bluetooth Basics. Viitattu 15.01.2018. https://learn.sparkfun.com/tutorials/bluetooth-basics

Swan M. 2012. Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. Viitattu 8.1.2018. http://www.mdpi.com/2224-2708/1/3/217/htm

Tibbo. 2017. Tibbo Project System (TPS). Viitattu 10.1.2018. http://tibbo.com/store/tps.html

Triggs Robert. 2017. All You Need To Know About NFC Tags. Viitattu 16.01.2018. https://www.androidauthority.com/nfc-tags-explained-271872/

Tucker Bowe. 2017. What is Bluetooth 5.0, And What Does It Mean For Your Next Pair Of Headphones?. Viitattu 15.01.2018. https://gearpatrol.com/2017/08/03/bluetooth-5-explained/

Wallenius Niklas. 2016. Miten pilvipalvelun tietoturva eroaa perinteisestä tietoturvasta. Viitattu 05.03.2018. https://niklaswallenius.fi/arkkitehtuuri/pilvipalvelun-tietoturva-erilainen/