
Älykodin kyberturvallisen järjestelmäintegraation suunnittelu ja toteutus

Diplomityö
Turun yliopisto
Teknillinen tiedekunta
Tietoliikennetekniikka
Maaliskuu 2023
Antti Hurtta

Tarkastajat:
Jouni Isoaho
Seppo Virtanen

ANTTI HURTTA: Älykodin kyberturvallisen järjestelmäintegraation suunnittelu ja toteutus

Diplomityö, 80 s.
Tietoliikennetekniikka
Maaliskuu 2023

Älykodit ovat yleistyneet viime vuosien aikana. Älylaitteista yleisimpiä ovat esimerkiksi valaisimet, robotti-imurit ja lukot. Yhä useampi älylaite vaatii myös jatkuvaa internetyhteyttä, mikä asettaa haasteita kotien kyberturvallisuudelle. Älykodin rakentamisen haasteina ovat myös useiden eri valmistajien omat, merkkikohtaiset järjestelmät. Jos käytössä on kolmen eri valmistajan älylaitteita, vaatii niiden käyttö todennäköisesti myös kolme eri sovellusta. Oman älykotijärjestelmän kokoamisella saavutetaan suurempi kyberturvallisuus ja useiden eri merkkisten laitteiden ohjaus yhdestä järjestelmästä.

Kyberturvallisuus on haaste älykotilaitteissa. Päivitysten heikko saatavuus ja vanhentuneet ohjelmistot tekevät laitteet alttiiksi kyberhyökkäyksille. Älykodin kyberturvallisuuden huomiointi korostuu, kun älylaitteet jatkavat yleistymistään. Jokainen lisätty laite, joka keskustelee ulkoisen kanssa, kasvattaa kyberhyökkäyksen kohteeksi joutumisen mahdollisuutta.

Tavoite diplomityössä on tutkia älykotijärjestelmien eroavaisuuksia ja toteuttaa näistä järjestelmistä yksi. Työssä esitellään älykodin periaatteita ja laitteistoa sekä määritellään ja toteutetaan turvallinen älykotijärjestelmä, jonka avulla älylaitteiden ohjaaminen on mahdollista. Järjestelmä hyödyntää useita eri tekniikoita, mahdollistaen erimerkkisten laitteiden käytön yhdessä. Myös itse kokoamalla tehdään älykotisopivia laitteita.

Diplomityön tuloksena toteutettiin toimintavarma ja kyberturvallinen älykotijärjestelmä, joka ei ole riippuvainen ulkoisen tarjoajan pilvipalvelusta. Havaittiin, että älykotijärjestelmissä on haasteita ja niihin löydettiin ratkaisuja. Valmistajien tuki älylaitteille saattaa olla hyvinkin lyhyt. Kyberturvallisuus todettiin suoraan internetiin kytketyissä laitteissa heikoksi, mutta sen parantaminen mahdolliseksi. Havaittiin myös, että älykotijärjestelmän käyttö vaatii jatkuvaa ylläpitoa.

Asiasanat: älykoti, internet of things, tietoturva, kyberturvallisuus, automaatio

Sisällys

1	Johdanto	1
1.1	Älykodin rakentamisen haasteet	2
1.2	Suunnitelma toteutukselle	4
1.3	Fyysinen turvallisuus	5
1.4	Tietoturva	6
2	Älykoti	7
2.1	Historia ja kehitys	7
2.2	Yksityisten turvallisuusalan yritysten tarjoamat valmisratkaisut, niiden vah- vuudet ja havaitut puutteet	9
2.3	Haasteet ja mahdollisuudet	10
2.4	Älykotiohjaimien vertailu	11
2.4.1	Home Assistant	12
2.4.2	Domoticz	13
2.4.3	OpenHAB	13
2.4.4	Älykotijärjestelmien erot	13
2.5	Tavoiteltavat hyödyt	14
3	Älykodin tietoliikenteen kyberturvallisuus	15
3.1	Yksityisyys	15
3.2	Suunnittelu ja periaatteet	16

3.3	Reitittimet ja palomuurit	16
3.4	Pilvipalveluiden riskit ja niiden hallinta	18
3.5	SSL/TLS-sertifikaatit	18
3.6	Monivaiheinen tunnistautuminen	19
3.6.1	Tekniikan esittely	19
3.6.2	Testaus ja toteutus	20
3.7	Kytkeytyminen verkkoon	22
3.7.1	VPN-esittely	22
3.7.2	Testaus ja toteutus	23
3.8	LAN-oikeus	24
3.9	HTTPS	24
3.9.1	Let's Encrypt	25
3.9.2	Dynaaminen nimipalvelin - Duck DNS	26
4	Järjestelmän määrittely ja toteutus	29
4.1	Käyttöliittymät	29
4.2	Järjestelmän määrittely	30
4.3	Yleiset älykotien kommunikaatioteknologiat	32
4.3.1	Langaton lähiverkko, Wi-Fi	32
4.3.2	Zigbee	32
4.3.3	Bluetooth	33
4.4	Valmiit laitteet ja niiden integrointi järjestelmään	33
4.4.1	Philips Hue -älyvalot	33
4.4.2	Amazon Alexa -älykotiapuri	34
4.4.3	Zigbee-laitteet	37
4.4.4	Wi-Fi-laitteet	42
4.5	Itse koottujen laitteiden tekeminen älykotisopiviksi ja niiden integrointi	44
4.5.1	Monivärinen LED-valonauha	44

4.5.2	Lämpötilamittari	45
4.5.3	Wi-Fi-älypistorasian modifointi	48
4.5.4	Ikean ilmanlaaduntunnistimen älyllistäminen	49
4.6	Älykotiarkkitehtuuri	52
4.6.1	Laitteiden toiminnan haittoina riippuvuus pilvipalvelusta	52
5	Testaus, havainnot ja pohdinta	54
5.1	Miten kyberturvallisuutta voisi vielä parantaa?	61
5.2	Laitteiden käyttötarkoituksia	62
5.3	Mitä havaittiin	63
5.4	Ongelmat ja parannusideat	66
5.5	Ajankohtaiset mahdollisuudet energian säästämiseksi	67
5.6	Muut huomiot	68
6	Yhteenveto	69
	Viitteet	72

Luku 1

Johdanto

Kotiemme tekniikka on muuttunut älykkäämmäksi. Nykyisin lähes yhdeksällä kymmenestä kotitaloudesta Suomessa on internetyhteys [1]. Tämä on osaltaan mahdollistanut älyratkaisujen läpilyönnin kodeissamme, sillä useat älykotilaitteet vaativat toimiakseen verkkoyhteyden. Yleisimpiä kotien älyratkaisuja ovat esimerkiksi älytelevisiot, älyvalot, älypistorasiat, erilaiset lämpötila-anturit ja valvontakamerat. Eräänlaisena älyratkaisuna voidaan pitää myös talojen etäluettavia sähkömittareita. Mittareiden avulla sähköyhtiön ja asiakkaan on mahdollista lukea kiinteistön ajantasainen sähkönkulutus, sillä niitä voidaan lukea myös etäyhteyden avulla [2]. Älykoti on laajentumassa myös kodinkoneisiin. Moni laite on mahdollista saada älykkäänä, verkkoon kytkettävänä versiona. Yleisimpiä älykkäitä kodinkoneita ovat pesukoneet, robotti-imurit ja uunit. Näiden laitteiden tietoturvapäivitysten jatkuminen on jopa valmistajille mysteeri [3]. Älykotiteknologioiden yleistymistä on kuitenkin hidastanut monimutkainen ja kallis arkkitehtuuri, laiteasennusten hankaluus, erilaisten verkkojen yhteentoimimattomuus, käyttämisen joustamattomuus sekä laitteiden käyttöönotosta syntyvä turvattomuus [4].

Laitteet kytkeytyvät erilaisiin älykotijärjestelmiin erilaisia protokollia hyödyntäen. Yleisimpiä näistä langattomista teknologioista ovat esimerkiksi Wi-Fi, Zigbee ja Bluetooth. Näitä tekniikoita esitellään tarkemmin luvussa 4.

Tutkielmassa suunnitellaan ja toteutetaan erilaisten laitteiden käytön yhdistämisen

mahdollistava älykotijärjestelmä, jonka avulla laitteiden käyttäminen on mahdollista yhdestä käyttöliittymästä. Lisäksi tässä diplomityössä muutetaan tavallisia laitteita älykäksi, ottaen huomioon myös niiden tietoturva.

1.1 Älykodin rakentamisen haasteet

Yksi suurimpia haasteita älykodin rakentamisessa on laitteiden yhteensopivuuden varmistaminen. Markkinoilla on useita eri valmistajia, jotka tuottavat laitteita omiin älykotijärjestelmiinsä. Eri valmistajien laitteiden välillä voi olla suuria eroja, ja tämän vuoksi kulluttajaa helpottaisi, jos hän voisi vapaasti yhdistellä haluamiaan laitteita yhdeksi kokonaisuudeksi. Tämä on toistaiseksi kuitenkin hankalaa, sillä laitevalmistajat haluavat saada käyttäjän sitoutumaan omaan palveluunsa ja laitteiden hankkimiseen. Poikkeuksiakin on, esimerkiksi Lidlin älykotituotteita on mahdollista yhdistää toimimaan Philips Hue [5]-järjestelmän kanssa. Philips Hue -järjestelmästä puhuttaessa tarkoitetaan käytännössä älyvalojen ohjaamista, sillä järjestelmä ei tue tällä hetkellä esimerkiksi lämpötila-antureita ja ovisensoreita. Yksi järjestelmä, joka sallii jo laajemmin erilaisten laitteiden yhdistämisen, on Samsungin SmartThings [6]. Tutkielmaa tehdessä havaittiin, että markkinoille tulee jatkuvasti uusia laitteita, joiden tietoturva on heikosti toteutettu. Näihin laitteisiin kohdistuvista hyökkäyksistä uutisoidaan usein.

Erilaisia haasteita älykodeille asettavat myös asunnon tyypit. Sillä, onko asunto vasta rakenteilla oleva omakotitalo, vai vuokralla oleva kerrostaloasunto, on vaikutusta älykodin mahdollisiin vaihtoehtoihin. Rakenteilla oleva omakotitalo tarjoaa vapaammat mahdollisuudet laitteistojen suunnittelulle ja asennuksille. Toimintavarmuuden parantaminen esimerkiksi kaapeloinnilla helpottuu merkittävästi, mikäli niitä on mahdollista tehdä jo rakennusvaiheessa talon rakenteisiin. Kerrostaloasunnossa asennusten kaapelointi voi olla jopa mahdotonta, jolloin laitteiden on toimittava langattomasti, mutta silti mahdollisimman toimintavarmasti. Tutkielmassa tullaan vertailemaan samalta vaikuttavia laitteita,

joilla kuitenkin on suuria eroavaisuuksia toisiinsa nähden.

Älykodin saamiseen oikeasti älykkääksi on esitetty useita mahdollisuuksia, esimerkiksi sumean logiikan (engl. fuzzy logic) [7], hermoverkkojen (engl. neural network) [8] ja Markov-verkkojen sijaintitiedon avulla [9].

Laitteiden käyttämisen tulisi olla mahdollisimman helppoa, joten kun käyttöliittymää suunnitellaan, pitää ottaa huomioon tämäkin seikka. Laitteiden jakaminen huoneittain tai laitetyypeittäin tekisi käytön helpommaksi. Esimerkiksi asunnon kaikkien valojen sammuttaminen yhdellä painikkeen painalluksella lisäisi käyttömukavuutta asunnosta poistuttaessa. Liiketunnistimien integroiminen järjestelmään luo asunnon valaistuksesta oikeasti älykästä, kun valaistus mukautuu asukkaan läsnäolon mukaan. Saavutettu lisähyöty tästä on valojen automaattinen sammuminen, mikä vähentää sähkönkulutusta.

Diplomityössä tullaan selvittämään vastaukset seuraaviin älykodin haasteisiin:

Tietoturva:

- Järjestelmän turvaaminen ulkopuolisilta hyökkäyksiltä
- Laitteiston toimivuus ilman internetyhteyttä
- IoT-järjestelmän heikon tietoturvan parantaminen

Laitteiden toiminnallisuuden yhdistäminen:

- Eri merkkisten laitteiden integroiminen yhteen järjestelmään
- Älykkäiden laitteiden keskinäinen kommunikaatio - liiketunnistimen ja valon yhdistelmä

Käytön helpottaminen:

- Laitteiden ohjaaminen yhdestä sovelluksesta tai verkkosivulta
- Automaatioiden luominen
- Langattomien painikkeiden sijoittaminen asuntoon vapaasti, haluttuihin paikkoihin

1.2 Suunnitelma toteutukselle

Diplomityössä tullaan toteuttamaan älykotijärjestelmä, joka pohjautuu avoimeen lähdekoodiin. Järjestelmä mahdollistaa älylaitteiden käytön paikallisesti, ilman riippuvuutta palveluntarjoajan tarjoamasta, mahdollisesti jopa maksullisesta pilvipalvelusta. Tarkoitus on hyödyntää avoimeen lähdekoodiin perustuvaa älykotialustaa, jonka avulla erimerkkisten laitteiden yhdistäminen yhdeksi kokonaisuudeksi tulee mahdolliseksi. Tavoitteena järjestelmällä on saada tietoa asunnon lämpötilasta, ilmankosteudesta ja ilmanlaadusta. Valaistusta tulee olla mahdollista säätää automaatioilla, langattomilla katkaisijoilla ja puheohjauksella. Myös kodissa olevista sensoreista, kuten ovimagneeteista ja vesivuotoantureista, tulee olla mahdollista vastaanottaa ilmoituksia käyttäjän älypuhelimeen.

Älykotijärjestelmä tullaan asentamaan palvelintietokoneelle, joka on käynnissä jatkuvasti. Älylaitteet tulevat kommunikoimaan suoraan tämän laitteen kautta, ilman tarvetta päästä ulkoverkkoon. Suurimpina hyötyinä tästä ovat saavutettu toimintavarmuus ja tietoturvallisuus. Työssä kuvataan, miten kaupasta ostetun laitteen ohjelmistoksi on mahdollista asentaa toinen, paikallisesti toimiva versio. Tämän ansiosta laite ei enää vaadi jatkuvaa internetyhteyttä, laite jatkaa toimimista, vaikka internetyhteys katkeaisikin jostain syystä.

Tutkielmassa tullaan vastaamaan seuraaviin haasteisiin:

- Toimivan älyvalaistuksen luominen:

- liikesensoreilla
- katkaisijoilla
- aikatauluilla

- Huoneilman seuraaminen:

- lämpötila
- ilmankosteus

- ilmanpaine
 - ilmanlaatu
- Laitteiden hyödyntäminen kodin hälytysjärjestelmänä:
 - ovisensori
 - palovaroitin
 - vesivuoto
 - valvontakamera
- Älykotiaivustajan käyttö ilmoitusten antamisessa ja valojen ohjauksessa
- Ilmoitusten toimitus halutulla tavalla käyttäjälle

Oletettuna lopputuloksena tutkielmassa on valmiiksi suunniteltu ja toteutettu älykoti-järjestelmä, joka toteuttaa edellä kuvatut toiminnot. Järjestelmä on tietoturvallinen ja toimintavakaa. Sen käyttö on helppoa ja mahdollista useilla erilaisilla laitteilla. Lisäksi tiettyjen laitteiden tietoturvaa tullaan parantamaan ohjelmistomuutosten avulla. Tutkielmassa tullaan myös suunnittelemaan ja toteuttamaan toimintoja automaatioiden avulla, esimerkiksi valaistuksen ohjaamista.

1.3 Fyysinen turvallisuus

Tutkielmassa toteutettavan älykodin avulla tullaan myös parantamaan kodin turvallisuutta. Tämä tullaan toteuttamaan valvontakameran ja erilaisten antureiden avulla. Esimerkiksi ovisensorin avulla voidaan tarkkailla sitä, onko joku kulkenut ovesta. Tähän lisäämällä liikeseensorin havainnot, saadaan hälytyksestä vielä varmempi. Termi *turvallisuus* kattaa muutakin, kuin murtautumisia asuntoon. Asumisen turvallisuutta tullaan parantamaan

asentamalla älypalovaroitin ja vesivuotoantureita pyykinpesu- ja tiskikoneiden alle. Näiden avulla on tarkoitus pystyä vastaanottamaan ilmoituksia asunnon mahdollisista poikkeustilanteista.

Turvallisuutta voitaisiin vielä lisätä älypalovaroittimella, joka savua havaitessaan antaisi käskyn sammuttaa sähköt kyseisestä huoneesta. Tämä jää kuitenkin tässä projektissa toteuttamatta kerrostaloasunnon vaatimien muutostöiden vuoksi. Älyvalaistuksen avulla olisi myös mahdollista lisätä esimerkiksi omakotitalon turvallisuutta. Asettamalla valaistukselle tietty rytmi, saadaan luotua vaikutelma, että asunnossa olisi joku. Tämä olisi kätevää esimerkiksi lomamatkojen aikana, kun halutaan luoda vaikutelma, että asunnossa ollaan kotona.

1.4 Tietoturva

Tutkielmassa toteutettavan järjestelmän tulee olla tietoturvallinen. Pääsy järjestelmään mahdollistaisi kodin ohjaamisen ulkoisen tahon toimesta. Tämä voisi muodostua asukkaita haittaavaksi, mikäli esimerkiksi valoja säädeltäisiin hallitsemattomasti jostain muualta. Vaarallisempaa tässä olisi, jos hyökkääjä pääsisi käyttäjän kotiverkkoon ja käsiksi siellä oleviin laitteisiin. Lisäksi kotiverkossa olevia laitteita olisi mahdollista hyödyntää muualla internetiin kohdistuviin hyökkäyksiin.

Tietoturvaan tullaan tutkielmassa kiinnittämään erityistä huomiota, ja näitä hyökkäyksille mahdollisia pisteitä pyritään minimoimaan. Lisäksi älykotijärjestelmään sisäänkirjautuminen tullaan toteuttamaan mahdollisimman turvallisesti, eikä vain käyttäjätunnuksen ja salasanan yhdistelmällä.

Tutkielmassa ratkaistaan yleisiä älykotiin liittyviä ongelmia toteuttamalla tietoturvallinen ja helppokäyttöinen älykotijärjestelmä. Tämän avulla älylaitteiden ohjaaminen on helppoa ja turvallista.

Luku 2

Älykoti

2.1 Historia ja kehitys

Termiä *älykoti* käytettiin ensimmäistä kertaa jo vuonna 1984 Amerikkalaiset kodinrakentajat -yhdistyksen toimesta. Termiä *langalliset kodit* oli tosin käytetty jo 1960-luvulla harrastelijoiden toimesta. Älykoti terminä määrittelee älyksi talon interaktiivisten teknologioiden toimimisen yhdessä. 1990-luvun aikana termi *älykoti* tuli laajemmin populaattuurin tietoisuuteen. Markkinat eivät ole kuitenkaan vielä silloin aktiivisesti panostaneet älykotien tutkimiseen, luomiseen tai kehittämiseen. [10]

Yleisiä, monille tuttuja sovellutuksia älykkäistä laitteista ovat esimerkiksi toimistotilojen liiketunnistimilla varustetut valaisimet. Nämä vapauttavat työntekijät valojen sammuttamisen vastuusta ja ovat varmatoimisia. Ainut haitta, joka toimistotyöntekijälle voit tästä tulla on, että valaisimet sammuvat liian herkästi, koska työ on usein paikallaan istumista. Tällöin liiketunnistin kuvittelee tilan olevan jo tyhjä ja sammuttaa valot pois.

Suomessakin on edellisen vuosituhanen lopulla ollut asunnoissa käytössä erilaisia rikosilmoitinjärjestelmiä [11]. Nämä sovellutukset tosin vaativat kiinteän kaapeloinnin toimiaukseen, joten tarpeet ja laitteiden sijainnit oli suunniteltava jo hyvissä ajoin rakennusvaiheessa. Nykyisin laitteistoja myyvät ja asentavat esimerkiksi yksityisen turvallisuusalan yritykset Sector Alarm ja Verisure. Laitteet ovat kehittyneet ja ovat kotitalouksissa

yleensä langattomasti toimivia. Laitteistoissa ja niiden toimintaperiaatteissa on suuriakin eroja, joita Ylen Kuningaskuluttaja on vertaillut hyvin [12].

Tutkielman kirjoittaja jäi pohtimaan, onko yritysten tarjoamien kameravalvontaratkaisujen tietoturvan taso lupauksien tasolla. Ulkopuolisen yrityksen kamera kuvaamassa kotia sisältä vuorokauden jokaisena hetkenä mietityttää varmasti useaa palvelua harkitsevaa asiakasta. Äskettäin uutisoitiin, että Ruotsin Verisuren työntekijät olisivat katselleet ja jakaneet käyttäjistä hälytyksien yhteydessä välittynyttä materiaalia, kuten alastonkuvia [13].

Gann, Barlow ja Venables [14] selvittivät eri tekijöitä älykotilaitteiden myynnin hiitaalle kasvulle. Viisi olennaisinta syytä, jotka he löysivät, olivat:

- Huono käyttäjän tarpeiden tietäminen
- Puutteellinen tieto saavutettavista hyödyistä ja mahdollisista riskeistä koskien mm. toimintavarmuutta ja tietoturvaa
- Standardien puutteesta johtuva integroinnin ja asennuksien haasteellisuus
- Laitteiden ja järjestelmien kalliit hinnat
- Epäkypsä teknologia, pelko laitteiden nopeasta vanhemisesta ja mahdollisesta päivitettävyydestä ja mukauttamisesta

Tutkijat mainitsivat, että on kuitenkin olemassa suuri ja kasvava potentiaali älykotien erilaisille teknologioille. Varsinkin ennustus lisääntyvästä kotona tehtävästä ostamisesta, pankkitoiminnoista, laskujen maksamisesta ja töiden tekemisestä osui täysin oikeaan. Nykyään nämä ovat laajalti käytössä ja etätyökin on lisääntynyt merkittävästi COVID-19-pandemian johdosta. Moni laitteista vaatii nykyään jatkuvaa, vakaata internetyhteyttä.

Clapper on esimerkiksi elokuvista tunnetuksi tullut eräänlainen älykodin laite. Se tuli markkinoille vuonna 1984 [15]. Clapper asetetaan pistorasiaan kytkettävän laitteen ja pistorasian väliin. Sen avulla käyttäjän on mahdollista käynnistää ja sammuttaa pistorasiassa olevia laitteita, kuten valoja, pelkällä käsien yhteen taputuksella.

Muita ensimmäisiä älykodin laitteiksi nykyäänkin luokiteltavia ovat mm. kameravalvonta, hälytinjaestelmät, lämmityksen ja viilennyksen säätö sekä valaistus. Olosuhteiden valvonta esimerkiksi lämpötilaa, ilmankosteutta ja ilmanlaatua mittaamalla on myös yleistä.

2.2 Yksityisten turvallisuusalan yritysten tarjoamat valmisratkaisut, niiden vahvuudet ja havaitut puutteet

Yritykset tarjoavat myös valmiita paketteja kodin hälytysjärjestelmiksi. Moderni hälytysjärjestelmä voi kattaa nykyään myös älykotilaitteiksi luokiteltavia komponentteja, kuten Sector Alarmin tarjoamia älypistorasioita ja vesivuotoilmaisimia [16]. Laitteiden ohjaaminen onnistuu Sector Alarm -sovelluksen avulla ja internetsivuilta löytyi maininta mahdollisuudesta kytkeä rasia pois päältä esimerkiksi hälytysjärjestelmän aktivoinnin yhteydessä. Laitteiston avulla pistorasioiden etäohjaus on mahdollista, mutta esimerkiksi rasian kytkeminen toimimaan jonkin toisen älykotijärjestelmän kanssa yhdessä ei ole mahdollista. Lisäksi myös Verisure tarjoaa vastaavia tuotteita älykotiin [17]. Sector Alarmin ja Verisuren järjestelmät kehittyvät kuitenkin nopeasti ja mahdollisuus laitteiston laajenemiselle ja mahdollisuuksien kasvamiselle on suuri. Esimerkiksi Sector Alarm tukee Yale-älylukkoja ja Verisurekin on alkanut tukea Arlo-valvontakameroita [16, 17]. Etuna näissä yritysten tarjoamissa järjestelmissä on palveluun sisältyvä vartiointipalvelu. Tämä tarkoittaa käytännössä sitä, että järjestelmän havaitessa poikkeuksia, on hälytyskeskuksella mahdollisuus lähettää vartija tarkastamaan kohde. Nämä vartijakäynnit ovat maksuttomia, sillä ne sisältyvät kuukausimaksuun. Hyöty tästä palvelusta korostuu mm. silloin, kun asukkaat ovat matkoilla ja koti on tyhjillään. Palvelu luo asiakkaalle mielenrauhaa, kun hälytyksen aiheellisuudesta saadaan varmistus. Aiheeton hälytys voi syntyä vaikkapa verhojen heilumisesta tai lemmikin liikkeistä kodin sisällä.

2.3 Haasteet ja mahdollisuudet

Älykodin rakentaminen on muodostunut haasteellisemmaksi sen mukaan, mitä enemmän uusia valmistajia ja laitteita on tullut myyntiin markkinoille. Jokaisella valmistajalla on omat älypuhelinsovelluksensa laitteidensa ohjaamiseen, jolloin käyttökokemuksesta tulee monimutkainen, kun jokaisella laitteella on oma sovelluksensa. Suuri hyöty keskittäytystä älykotijärjestelmästä on, että kaikkien eri sovellusten toiminnallisuus voidaan saavuttaa vain yhdellä sovelluksella. Toinen hyöty tästä on, että eri merkkiset laitteet voidaan yhdistää keskustelemaan saumattomasti toistensa kanssa. Valmistajan X valokytin voidaan määrittää ohjaamaan valmistajan Y valoa. Tämä avaa myös paljon mahdollisuuksia älykodin kehittämiseksi, eivätkä teennäiset sovellusrajoitukset muodostu ylittämättömiksi. Lisäksi riippumattomuus pilvipalvelusta estää internetyhteyden katketessa koko talon muuttumisen ohjaamattomaksi. Myös yksityisdata säilyisi edelleen käyttäjän kotona, ilman kaiken tiedon tallentumista pilvipalveluun.

Toinen haaste projektissa tulee olemaan saavutettavissa olevien älyratkaisuiden toteuttaminen mahdollisimman laajasti kerrostaloasunnossa. Esimerkiksi lämmityksen ja viilennyksen säätäminen on hyvin rajattua. Tältä osin tutkimuksessa pääpaino tulee keskittymään enemmän ilman monitorointiin, kuin itse säätämiseen. Valaistukseen on mahdollista vaikuttaa vaihtamalla nykyiset polttimot älykkäiksi. Älylamppuja on nykyään saatavilla useilla eri kannoilla, poikkeuksena esimerkiksi kylpyhuoneen peilikaapin loisteputki. Langattomien ovisensoreiden avulla on mahdollista tarkkailla esimerkiksi onko ulko-ovi auki vai kiinni. Langallisten antureiden avulla toimintavarmuus paranisi, mutta todettiin johdotuksien jälkiasennus kerrostaloasunnossa mahdottomaksi. *Zigbee*-tekniikkaan päätyminen oli luonnollista, koska laitteiden hinta ja saatavuus olivat hyviä. Lisäksi nämä laitteet toimivat irrallisina eivätkä kuormita kodin Wi-Fi-verkkoa. Modernit langattomat tukiasemat tukevat nykyään vakaasti jopa useita kymmeniä Wi-Fi-laitteita, mutta silti tavoiteltavampaa olisi saada säästettyä verkon kapasiteettia sitä enemmän vaativille laitteille, kuten tietokoneille. Lisäksi *Zigbee*-laitteet ovat tehokkaita ja kuluttavat vähän energiaa

verrattuna Wi-Fi-laitteisiin. Mikäli käyttäjä joutuisi jatkuvasti pitämään kirjaa laitteidensa paristojen tasosta ja vaihtelemaan niitä toistuvasti, muodostuisi se älykodin rasitteeksi.

Kolmas haaste projektissa tulee olemaan järjestelmän saaminen toimintavarmaksi ja varatoiminnallisuuden turvaaminen. Tavoitteena on, että esimerkiksi asunnon valaistusta olisi mahdollista säätää kahdella eri tavalla, mikäli järjestelmä ei jostain syystä toimitakaan. Toimintavarmuutta pyritään myös parantamaan ajastamalla automaattiset varmuuskopiot päivittäin. Täten äkillisen virhetilan ilmaantuessa olisi mahdollista nopeasti palauttaa edellinen toimiva konfiguraatio järjestelmästä. Lisäksi virtuaalikoneen avulla on mahdollista kaapata täydellinen varmuuskopio senhetkisestä tilasta, esimerkiksi ennen järjestelmän päivittämistä. Varmuuskopion avulla on mahdollista palauttaa edellinen, toimiva versio vain yhdellä klikkauksella, mikäli päivityksen yhteydessä tulisi virhe. Valaistus on oleellinen osa kodin tekniikkaa, ja tähän kiinnitettiin erityistä huomiota varmistamalla valaistuksen toimivuus myös internetyhteyden katkoksen aikana.

Ympäri vuorokautinen internetyhteys luo myös mahdollisuuden kyberhyökkäykselle mistä päin maailmaa tahansa. Tämän vuoksi salasanojen on oltava erittäin vahvoja. Tulee myös selvittää muiden lisävahvennuksien käyttöönoton mahdollisuuksia. Portin avaaminen omasta reitittimestä ulkoverkkoon lisää aina mahdollisuutta joutua tietomurron kohteeksi. Riskien tiedostaminen onkin tärkeä osa projektin toteuttamista, sillä tietoturvallisuuden tulee olla korkealla tasolla.

2.4 Älykotiohjaimien vertailu

Älykotien ohjaamiseen tarkoitettuja alustoja on nykyään useita. Yleisimpinä näistä voidaan pitää Applen Homekitiä [18], Amazon Alexaa [19] ja Google Homea [20]. Moni kuluttaja valitsee laitteensa yhteensopivuuden näiden alustojen mukaan. Silti useat älykotiharrastajat haluavat vapaammin valita laitteidensa merkit ja yhdistellä niitä mielekseen kokonaisuudeksi. Tähän tarkoitukseen on kehitetty avoimeen lähdekoodiin pe-

rustuvia älykotiratkaisuja. Tunnetuimmat näistä ovat Home Assistant [21], Domoticz [22] ja OpenHAB [23]. Näiden avulla kuluttaja voi itse yhdistää erimerkkiset laitteet yhteen ja saada laitteet keskustelemaan keskenään ilman rajoituksia. Tämä laajentaa älykodin mahdollisuuksia merkittävästi, koska esimerkiksi Philips Hue -järjestelmä ei tue suoraan magneettisia oviantureita, jotka ohjaisivat valaistusta. Älykotiohjaimen avulla tämä on mahdollista saavuttaa ohjaamalla laitteita keskiteysti samasta järjestelmästä. Helpoin tapa päästä alkuun oman älykotijärjestelmän rakentamisessa on asentaa jokin näistä mainituista ohjelmistoista Raspberry Pi -koneelle [24], jotka ovat huokeampia kuin normaalit tietokoneet. Laitteisto on riittävän tehokas suorittamaan älykotiohjaimien vaatimaa ohjelmistoa.

2.4.1 Home Assistant

Paulus Schoutsen alkoi kehittää Home Assistantia vuonna 2013. Projekti alkoi alunperin yksinkertaisesta Python-skriptistä valojen ohjaamista varten. Home Assistantia ajavassa laitteessa ei ole vakiona yleensä radioita, vaan käyttäjä voi itse valita tarpeelliseksi kokemansa radiot, USB-tikkuja käyttäen. [21, 25] Sen toiminta perustuu Python 3 -backendiin ja Polymeriin frontendin osalta. Automaatio ja konfigurointi pohjautuvat YAML-kieleen, tosin uusimmissa versioissa suuri osa konfiguroinneista on mahdollista tehdä myös graafista käyttöliittymää hyödyntäen.

Home Assistantin eduiksi voidaan katsoa:

- Helppo käyttöönotto askeleittain
- Mitään käyttäjädataa ei tallenneta pilveen
- Kaikki koodi on avointa Githubissa
- Automaatiosääntöjä voi muokata mieleiseksi monella eri tavalla
- Aktiivisen yhteisön tuki mahdollisten ongelmien selvittelyssä

Kaikissa järjestelmissä on myös heikkouksia. Home Assistantissa näitä ovat esimerkiksi YAML-kielen opettelun tarve ja kirjoitusasun tarkkuudesta johtuva konfiguraatiovirheiden mahdollisuus.

2.4.2 Domoticz

Domoticz [22] on kevyempi järjestelmä. Se on kuitenkin jo ikääntynyt, mikä näkyy mm. käyttöliittymän vanhanaikaisena ulkoasuna. Lisäksi kotisivulla oleva yläpalkin ”Manual”-valikko ohjaa ohjedokumenttiin, jonka päiväys on vuodelta 2015. Järjestelmää kehitetään kuitenkin jatkuvasti ja päivityksiä julkaistaan. Silti dokumentaatio vaikuttaa osittain vanhentuneelta ja ongelmiin voi olla hankala löytää vastauksia. Domoticzin etuna Home Assistantiin ja OpenHABiin verrattuna on järjestelmän keveys. Järjestelmä on myös hyvin vakaa, mutta tuki erilaisille laitteille on rajoitetumpi, kuin Home Assistantissa ja seuraavassa kappaleessa esiteltävässä OpenHAB:ssa.

2.4.3 OpenHAB

OpenHAB [23] on myös eräs suosittu älykotiohjain. Laitteiden lisääminen on tähän järjestelmään haastellisempaa, kuin Home Assistantissa. Aluksi valittava käyttöliittymä vaikuttaa myös itse OpenHAB:n ominaisuuksiin. Valittu näkymä saattaa rajoittaa esimerkiksi automaatioiden toiminnallisuutta ilman, että käyttäjää informoidaan tästä. Home Assistantissa sen sijaan on vain yksi yhteinen käyttöliittymä, johon on mahdollista asentaa erilaisia teemoja ja muokattuja kortteja. Käyttäminen aloittelijoillekin on tehty helpoksi ja lisäosilla järjestelmää on mahdollista laajentaa suuremmaksi kokonaisuudeksi.

2.4.4 Älykotijärjestelmien erot

Ensimmäiset vertailukriteerit olivat käytön helppouden arviointi ja ulkoasun sopivuuden varmistaminen. Näistä Home Assistant teki alkuun vaikutuksen modernilla ulkonäöllään

verrattuna kahteen edellämainittuun vaihtoehtoon. Esimerkiksi Domoticzin käyttöliittymä vaikuttaa jo hieman vanhentuneelta ikonien ja ulkoasun osalta. Home Assistantin ensimmäisen käynnistyksen yhteydessä tehtävä ”onboarding” etsii automaattisesti kotoa löytyviä älylaitteita. Esimerkiksi Philips Hue -valot löytyivät nopeasti. Valmiiden integraatioiden vuoksi Home Assistant ja OpenHAB erottuivat selkeästi. Molemmat järjestelmät tukevat tuhansien eri valmistajien laitteiden lisäämistä järjestelmiinsä. Domoticzistä oli hankala löytää etuja muihin verrattuna. Näistä syistä Home Assistant on varteenotettava vaihtoehto tutkielmassa käytettäväksi älykotijärjestelmäksi.

2.5 Tavoiteltavat hyödyt

Suunniteltavan ja toteutettavan järjestelmän tavoitteena on helppokäyttöisyys ja useiden erimerkkisten laitteiden integrointi. Järjestelmän avulla kerättävä data jäisi suurelta osin järjestelmän sisälle, eikä välittyisi eteenpäin palveluntarjoajille. Kerätyn datan esittäminen tulisi olla selkeää ja ymmärrettävää, erilaisia graafisia vaihtoehtoja hyödyntäen.

Valaistuksen tavoitteena on saada lisättyä älykkäitä automaatioita ja liikkeeseen perustuvaa reagointia. Valojen syttyminen tiettyyn kellonaikaan, auringon asennon mukaan, liiketunnistimella tai ovianturilla olisi tavoiteltava hyöty. Toteutettavan järjestelmän tavoite on saada yhdistettyä erimerkkiset laitteet toimimaan yhdessä toistensa kanssa, esimerkiksi Sonoffin valmistama ovimagneetti sytyttäisi Lidlin älypistorian avulla valot eteiseen, kun ovi avataan.

Tärkein hyöty järjestelmästä on saavuttaa korkeampi tietoturvallisuus. Esimerkiksi mahdolliset valvontakamerat toimisivat ilman jatkuvaa internetyhteyttä, vain sisäverkon sisällä. Langattomaan lähiverkkoon kytkeytyvät laitteet tulisi saada toimimaan ilman riippuvuutta valmistajan pilvipalvelusta. Laitteiden integroinnin yksi hyödyistä olisi päästä käyttämään vain yhtä sovellusta kaikkien laitteiden ohjaamiseen, esimerkiksi älypuhelimella.

Luku 3

Älykodin tietoliikenteen kyberturvallisuus

Järjestelmää suunniteltaessa päätettiin keskittyä tekemään siitä myös mahdollisimman tietoturvallinen. Kaikkein turvallisın tapa olisi ollut jättää järjestelmä toimimaan täysin vain sisäverkossa, näin järjestelmä olisi ollut täysin irrallaan internetistä. Porttejakaan ei olisi ollut tarpeellista avata reitittimestä ulkoverkkoon. Lopulta haluttiin kuitenkin päästä tarkkailemaan järjestelmää etänä ja saamaan siitä ilmoituksia silloinkin, kun käyttäjä ei ole kotona. Onneksi turvallisen yhteyden luomiseen on olemassa kuitenkin useita eri tapoja, joita esitellään luvun loppuosassa tarkemmin.

3.1 Yksityisyys

Monen muunkin palvelun siirtyessä kybermaailmaan tulisi pohtia myös näiden palvelujen turvallisuutta. Mikäli kodissa sijaitsevilla laitteilla luodaan yhteyksiä esimerkiksi lääkäreiden vastaanotoille, tulisi näiden laitteiden olla tietoturvallisia ja päivitettyjä. Harkke, Alessi ja Collan esittivät, että yksityisyyslakeja tulisi mukauttaa näiden uusien teknologioiden mukaisiksi, jotta potilastiedot pysyisivät turvattuina [26]. Laitteiden kytkeminen internetiin lisää aina käyttäjän riskiä joutua tietomurron kohteeksi.

Kyberhyökkäyksellä on mahdollista saavuttaa pankkitietojen, käyttäytymisen, osoitetietojen, käyttäytymistapojen ja ostoskäyttäytymisen vuotaminen väärin käsiin [27]. Lisäksi vaarantuneita IoT-laitteita (engl. internet of things), kuten reitittimiä, on mahdollista hyväksikäyttää troijalaisen avulla esimerkiksi roskapostin lähettämiseen [28].

Esineiden internetillä (IoT) tarkoitetaan avointa ja kattavaa verkkoa älykkäistä objekteista, joiden on mahdollista järjestäytyä itsekseen, jakaa informaatiota ja reagoida tilanteiden ja ympäristön muutoksiin. [29]

3.2 Suunnittelu ja periaatteet

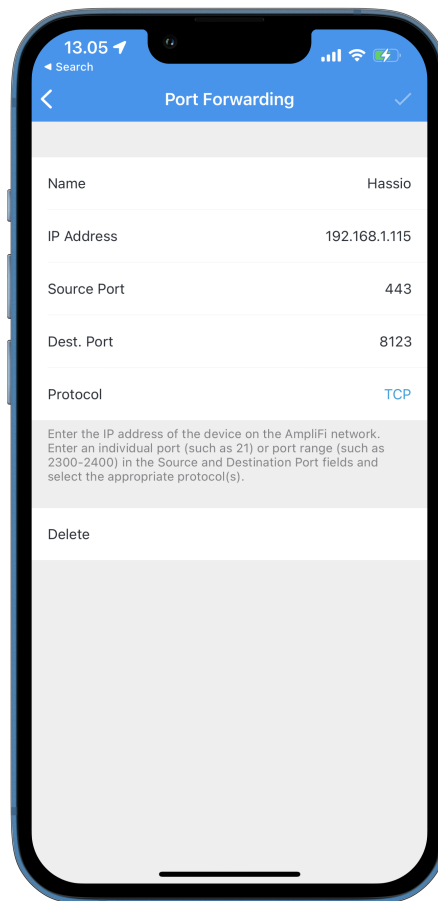
Olennaisinta tietoturvassa on huolehtia mahdollisten ohjelmistopäivitysten asentamisesta. Peruskäyttäjät päivittää reitittimensä ohjelmistoa harvoin, vaikka valmistaja todennäköisesti päivittyisi näihin tekisiikin. Usein reititin asennetaan vain kerran, käyttöönoton yhteydessä ja tämän jälkeen annetaan laitteen vain olla käytössä. Myös IoT-laitteita tulisi jatkuvasti päivittää. Päivitys on mahdollista helposti esimerkiksi langattomilla OTA-päivityksillä (engl. over-the-air) [30]. Älykotijärjestelmää suunniteltaessa haluttiin ottaa huomioon myös tämä seikka, joten reitittimeksi valittiin laite, jonka päivittäminen olisi mahdollisimman helppoa.

3.3 Reitittimet ja palomuurit

Reitittimeksi haluttiin valita toimintavarma ja tietoturvallinen vaihtoehto, ja siksi valittiin Unifin AmplifiHD-reititin [31], jossa on sisäänrakennettuna mm. palomuri ja VPN yhteys. Laitteen päivittäminen on helppoa etupaneelissa sijaitsevan kosketusnäytön kautta. Laite ilmoittaa saatavilla olevasta päivityksestä automaattisesti ja käyttäjän täytyy vain koskettaa asennuspainiketta näytöstä. Viimeisin päivitys laitteelle tuli syyskuussa 2022, mikä oli merkittävä seikka jo vuonna 2016 julkaistussa laitteessa. Laitteen elinajan pitkän tuen varmuus olikin tärkeä syy laitteen valintaan. Uusin päivitys toi myös tuen kolmannen

langattoman verkon luonnille, varsinkin IoT-laitteita varten.

Home Assistantin ulkoverkosta käyttämisen vaatimus on porttiavaus reitittimestä ulkoverkkoon, jonka suorittamista havainnollistetaan kuvassa 3.1.



Kuva 3.1: Portin avaaminen AmplifiHD-reitittimestä

Seuraava kehitysaskel verkon turvallisuuden parantamiseksi voisi tulevaisuudessa olla pfSense-palomuurin [32] toteuttaminen. Se olisi avoimeen lähdekoodiin perustuva ratkaisu ja laitteiston voisi itse valita mieleisekseen. Tämä mahdollistaisi paljon laajemman määritysten asettamisen verkkoon ja erilaisten aliverkkojen luonnin. Mikäli joitain IoT-laitteita ei saada kommunikoidaan suoraan Home Assistantin kautta, niin olisi hyvä saada nämä internetiin kytketyt laitteet omaan verkkoonsa, josta ei olisi pääsyä itse kotiverk-

koon. Vaikka älykotilaite vaarantuisikin ja mahdollisesti hakkeri saisi pääsyn laitteeseen, sen avulla ei onnistuttaisi kuitenkaan saavuttamaan pääsyä käyttäjän kotiverkkoon verkkojen eriyttämisen ansiosta.

Saavutettu lisähyöty erillisissä verkoissa on myös käyttäjäkohtainen konfigurointi. Oma Wi-Fi-verkko (SSID) voitaisiin luoda esimerkiksi myös vieraita, työtietokoneita tai vaikka lapsia varten, IoT-laitteiden lisäksi. Tämän avulla on mahdollista rajoittaa laitteisiin käsiksi pääsyä niin laitetasolla, kuin myös ajallisestikin. Langattomissa verkoissa korostuu turvallisuuden harkitseminen enemmän, kuin langallisten laitteiden kytkemisessä kotiverkkoon.

3.4 Pilvipalveluiden riskit ja niiden hallinta

Pilvipalvelut tuovat mukanaan aina tietoturvaan liittyviä riskejä. Kun käyttäjä liittyy johonkin pilvipalveluun, hänestä aletaan kerätä dataa esimerkiksi käytöksen perusteella. Miten käyttäjä hyödyntää palvelua tai laitettaan? Mitä hän ostaa palvelusta? Millaista dataa käyttäjä syöttää palveluun? Tämä kaikki on erittäin arvokasta tietoa pilvipalvelun tarjoajille. Onkin olemassa hyvä sanonta: ”jos palvelu on sinulle ilmainen, olet silloin tuote”. Usein palvelun ilmaiskäyttö onkin mahdollista käyttäjistä myytävän datan vuoksi. Käyttäjät eivät useinkaan tiedosta, että monet nimellisesti ilmaisupalvelut, kuten Gmail ja Facebook ovat kalliita ylläpitää, datakeskukset ja verkkoyhteydet vaativat rahaa, joten suuri osa käyttäjistä saatavista tiedoista kaupataan eteenpäin, jotta palvelut pysyisivät ilmaisina [33]. Tästä käyttäjästä saatavasta datasta käytetään myös lyhennettä PII (engl. Personally Identifiable Information).

3.5 SSL/TLS-sertifikaatit

Internetsivun identiteetin varmistaminen ja suojatun yhteyden muodostaminen on mahdollista SSL sertifikaatin avulla. Lyhenne SSL tulee sanoista Secure Sockets Layer. Tällä

tarkoitetaan suojatun yhteyden muodostamista verkkopalvelimen ja internetselaimen välille. Tämän avulla näiden välillä kulkeva tieto pysyy salattuna. Nykyään käytössä on TLS (engl. Transport Layer Security), joka on seuraaja jo vanhentuneelle SSL:lle.

Certificate Authority, lyhennettynä ”CA”, eli varmentaja on se taho, joka myöntää varmenteen. CA:ta voidaan pitää PKI:n (engl. Public Key Infrastructure) perustana, sillä se on ainut taho, joka voi myöntää sertifikaatteja. [34]

Suojattua yhteyttä voidaan kutsua nykyään alan standardiksi, sillä oletuksena on, että sivustot käyttävät aina salattua yhteyttä kommunikoinnissa. Käyttäjä tunnistaa tämän helpon selaimen osoitepalkin läheisyydessä sijaitsevasta lukosta, joka on esitetty myös kuvassa 3.6. Lisää turvatun yhteyden luomisesta älykotipalvelimen ja käyttäjän välille tullaan esittelemään kappaleessa 3.9.

3.6 Monivaiheinen tunnistautuminen

3.6.1 Tekniikan esittely

Turvallisuutta lisättiin ottamalla käyttöön monivaiheinen tunnistautuminen (engl. multi-factor authentication, lyhennettynä MFA tästä eteenpäin). Monivaiheinen tunnistautuminen on metodi, jolla käyttäjä voidaan tunnistaa kahden tai useamman yksittäisen tunnistautumismenetelmän avulla [35]. Tämä mahdollistaa turvallisemman kirjautumisen palveluun. Yleisin tapa toteuttaa tämä on salasanan ja puhelimeen saatavan koodin yhdistelmä [36]. Koodi on usein mahdollista saada SMS:n kautta, mutta autentikointisovellusten käyttö on yleistymässä. Näitä käytettäessä käyttäjä syöttää ensin kirjautumissivulle salasanan. Mikäli salasana todetaan oikeaksi, käyttäjälle avautuu seuraava ikkuna, johon tulee syöttää toisen vaiheen koodi. Kun molemmat on hyväksytty oikeiksi, käyttäjä pääsee kirjautumaan palveluun onnistuneesti.

Tunnistautumismenetelmiä voidaan jaotella esimerkiksi taulukon 3.1 mukaisesti.

Kaksivaiheinen tunnistautuminen yhdistää kaksi näistä menetelmistä ja tätä pidetään siksi

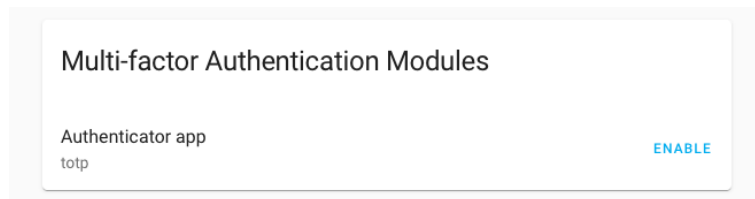
Metodi	Esimerkiksi	Ominaisuudet
Mitä muistat:	Tunnusluku, salasana, PIN-koodi jne.	Mahdollista jakaa ja unohtaa
Mitä omistat:	Avaimet, pankkikortit, kulkulätkät jne.	Mahdollista jakaa ja kopioida
Mitä sinussa on:	Sormenjälki, kasvot, iiris jne.	Ei mahdollista jakaa

Taulukko 3.1: Olemassa olevat käyttäjän tunnistamismenetelmät [37]

vahvempana ja turvallisempana kuin vain yhden menetelmän käyttöä [36].

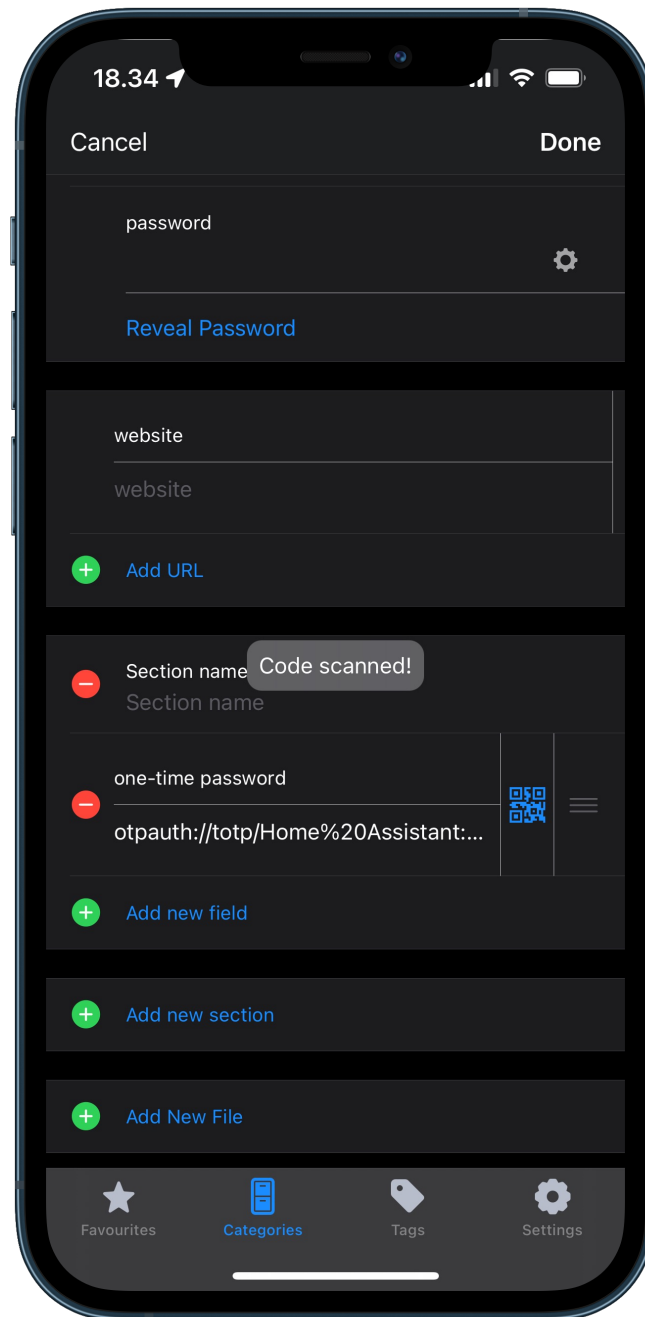
3.6.2 Testaus ja toteutus

Monivaiheinen tunnistus toteutettiin Home Assistantissa kirjautumalla sisään omalla profiililla ja sen asetuksista aktivoimalla tunnistautuminen käyttöön. Kuvassa 3.2 on esitelty käyttöönoton aloittaminen.



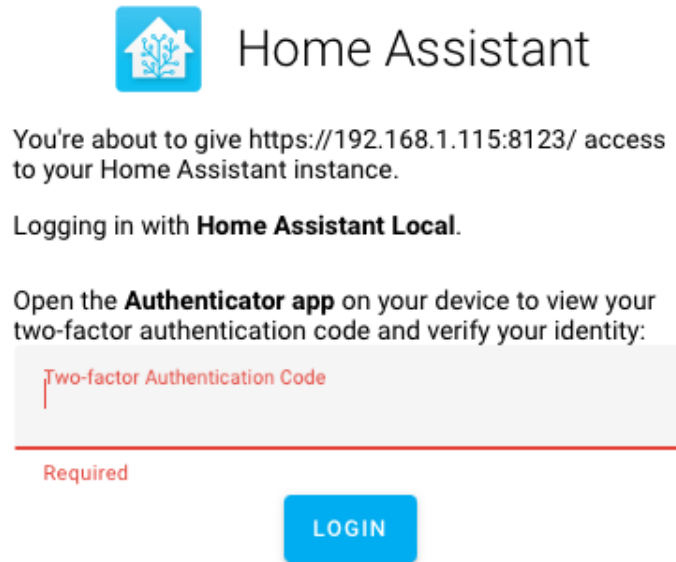
Kuva 3.2: Monivaiheisen autentikoinnin käyttöönotto

Kuvassa 3.3 generoitu QR-koodi luettiin puhelimen 1Password-sovelluksella.



Kuva 3.3: QR-koodi luettuna puhelimen salasanojenhallintasovelluksella

Home Assistant ja salasanasovellus saatiin onnistuneesti yhdistettyä. Jatkossa kirjautuminen vaatii aina salasanan lisäksi muuttuvan kuusinumeroisen koodin 1Password-sovelluksesta. Kirjautuminen vaatimassa koodia kuvassa 3.4.



The screenshot shows the Home Assistant login interface. At the top is the Home Assistant logo (a blue house with a white plant) and the text "Home Assistant". Below this, it says "You're about to give https://192.168.1.115:8123/ access to your Home Assistant instance." and "Logging in with Home Assistant Local." The main instruction is "Open the **Authenticator app** on your device to view your two-factor authentication code and verify your identity:". Below this is a text input field with the placeholder "Two-factor Authentication Code" in red. A red line is drawn across the field, and the word "Required" is written in red below the line. At the bottom right is a blue button with the text "LOGIN" in white.

Kuva 3.4: Kirjautumissivu pyytämässä vaadittavaa koodia

3.7 Kytkeytyminen verkkoon

3.7.1 VPN-esittely

VPN-tunneleita (engl. Virtual Private Network) käytetään ylläpitämään verkkoyhteyden kautta jaetun datan yksityisyyttä pakettitason salauksella, joka tekee VPN:n kautta toimivien palveluiden tunnistamisen erittäin hankalaksi [38]. Vaikka intranet käyttää interneettiä, näiden protokollat on pidetty tarkoin erillään. Protokollan avulla on myös mahdollista autentikointi ja kryptaus [39]. Tämän avulla liikenne on mahdollista salata siten, että esimerkiksi julkisessa Wi-Fi-verkossakin liikenne pysyy salattuna.

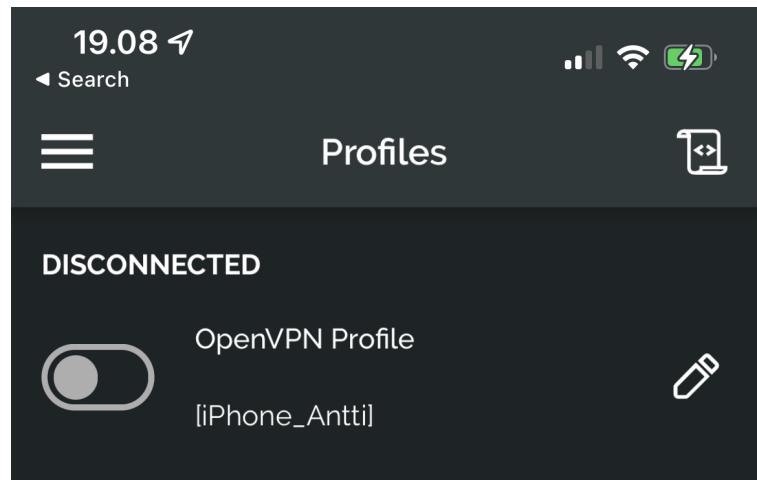
3.7.2 Testaus ja toteutus

Tietoturvallisuuden parannusmahdollisuuksia pohdittaessa päädyttiin kokeilemaan myös VPN-yhteyden kautta yhteyden muodostamista. Tämä mahdollisti vielä turvallisemman yhteydenottotavan, mutta esteeksi käytölle muodostui jokaisella käyttökerralla vaadittava erillinen yhteyden käynnistys, käytön hitaus sekä ilmoitusten vastaanoton vaikeus. VPN-yhteyden kautta järjestelmästä saatavien push-ilmoitusten vastaanotto on mahdollista vain, kun yhteys on aktiivinen. Tämä vaatisi jatkuvaa VPN-yhteyttä järjestelmään, joka lisäisi älypuhelimien akun käyttöä sekä hidastaisi muuta internetliikennettä.

Testaus toteutettiin käyttämällä avoimeen lähdekoodiin perustuvia ratkaisuja. Perens on määritellyt termin *avoin lähdekoodi* [40]. Tiivistettynä termi tarkoittaa ilmaiseksi käytettävää ja sen koodin sisältö on avointa luettavaa kaikille. Etuna tässä on laaja käyttäjäkunta ja yhteisön tuki mahdollisten ongelmien esiintyessä.

Kokeilussa luotiin Ubuntu server -virtuaalikone Proxmox-alustalle. Kyseiseen virtuaalikoneeseen asennettiin vaadittavat OpenVPN-paketit [41]. Asennuksen yhteydessä luodaan tiedosto, jonka avulla VPN-tunnelin avaaminen tulee mahdolliseksi. Tämän tiedoston avaamiseen tarvitaan haluttu VPN-ohjelma, tähän valittiin virallinen OpenVPN-sovellus. Kyseinen luotu tiedosto tulisi saada siirrettyä laitteeseen mahdollisimman turvallisesti. Esimerkiksi sähköpostilla lähettämistä ei suositella. Yhteyden muodostaminen on käyttäjästävällistä vain yhden painalluksen takia. Kuvassa 3.5 esitellään OpenVPN-sovelluksen käyttöliittymää iPhonella.

Onnistuneen yhteydenmuodostamisen jälkeen Home Assistantin sovellusta tai sivustoa on mahdollista käyttää ns. paikallisesti, vaikkei käyttäjä olisikaan samassa kotiverkossa. Tämä tapa käyttää sovellusta olisi erittäin tietoturvallinen, sillä järjestelmään pääsyyn vaaditaan pääsy joko käyttäjän kotiverkkoon tai kyseinen VPN-konfigurointitiedosto, jonka avulla pääsy myönnetään. Tämä tapa on kuitenkin hankalampi toteuttaa, mikäli päätelaitteita käyttämiseen on useita. Tällöin jokaiselle laitteelle tulisi luoda uusi tiedosto ja siirtää se turvallisesti laitteeseen. Mikäli laite katoaisi, olisi mahdollista evätä vain tuon



Kuva 3.5: VPN yhteyden käynnistäminen puhelinsovelluksella. Painike vasemmalla.

kyseisen laitteen pääsy VPN-yhteyteen.

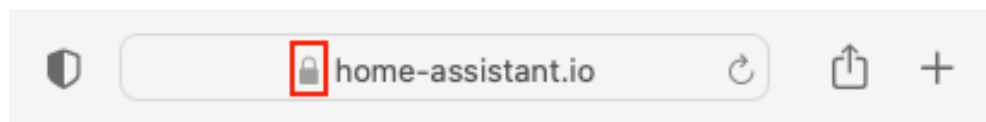
3.8 LAN-oikeus

Yksi mahdollisuus järjestelmän käyttämiselle ja ohjaamiselle olisi sallia vain paikallinen käyttö. Tällöin ohjaaminen ja monitorointi tapahtuisi vain käytettävästä kotiverkosta. Tämä olisi varmasti riittävää monelle käyttäjälle. Järjestelmän toiminnallisuus olisi mahdollista säilyttää samana, valojen liiketunnistukset, automaatiot ja muut mahdolliset älyratkaisut toimisivat normaalisti. Ainut menetetty toiminnallisuus olisi järjestelmän käyttö muualta, kuin kotoa. Mikäli käyttäjä ei koe tarpeelliseksi päästä käsiksi tietoihin etänä, olisi tämä tietoturvallinen ja toimiva ratkaisu.

3.9 HTTPS

Vaihtehto, johon tutkielmassa lopulta päädyttiin, oli avata portti ulkoverkkoon kuten kuvassa 3.1, jonka kautta pääsy järjestelmään tuli mahdolliseksi. Tämä oli tutkimisen lopputuloksena paras kompromissi tietoturvan ja helppokäyttöisyyden välillä. Nyt Home Assistant -sovelluksen avaaminen tuo esiin saman näkymän, riippumatta siitä onko laite ko-

tiverkossa, vieras-Wi-Fi:ssä tai mahdollisesti mobiiliverkossa. Turvatus HTTPS-yhteyden luominen muodostui olennaiseksi. Ero normaaliin HTTP:en on se, että HTTPS on turvallisempi. Artikkelissaan *The Cost of the "S" in HTTPS*, Naylor ym. kuvailevat että ”HTTPS todentaa viestinnän päätepiisteet ja tarjoaa luottamuksellisuutta jatkuvalle tiedonsiirrolle” [42]. Helpoiten käyttäjä tunnistaa turvatus HTTPS-yhteyden osoitepalkin lulkolta näyttävästä kuvakkeesta kuvassa 3.6. Tämä on erittäin selkeä tapa kuvata käyttäjälle



Kuva 3.6: Safari-selaimen osoitepalkki, jossa HTTPS-yhteys ilmaistaan lukolla

sivuston turvallisuuden olevan toivotulla tasolla.

Pitkällisen tutkimustyön tuloksena löytyi Let's Encrypt [43]-niminen palvelu. Se on avoin, ilmainen ja automatisoitu HTTPS-varmennepalvelun tarjoaja, CA (engl. certificate authority). Se on perustettu vuonna 2015 ja on siitä lähtien kasvanut maailman suurimmaksi HTTPS-varmenteiden takaajaksi. Tästä enemmän seuraavassa kappaleessa.

3.9.1 Let's Encrypt

Suojatus HTTPS-yhteyden luominen käyttäjän laitteen ja Home Assistantin välille vaatii toimiakseen sertifikaatin. Tämän vuoksi valittiin käytettäväksi Let's Encrypt -palvelua. Se jakaa käyttäjille digitaalisia sertifikaatteja, joita tarvitaan HTTPS-yhteyden mahdollistamiseksi verkkosivustoille [44]. Tutkielman tekemisen aikana on tullut mahdolliseksi ottaa Let's Encrypt käyttöön Duck DNS -lisäosan mukana, joten turvallisuuden lisäämisen kynnys on madaltunut entisestään. Tämä tapa helpottaa entisestään sen käyttöönottoa. Lisää Let's Encrypt -palvelun toiminnasta voi lukea sivustolta [45]. Tärkeä huomio on se, että turvallisuuden lisääminen on käyttäjälle täysin ilmaista ja erittäin suositeltavaa.

3.9.2 Dynaaminen nimipalvelin - Duck DNS

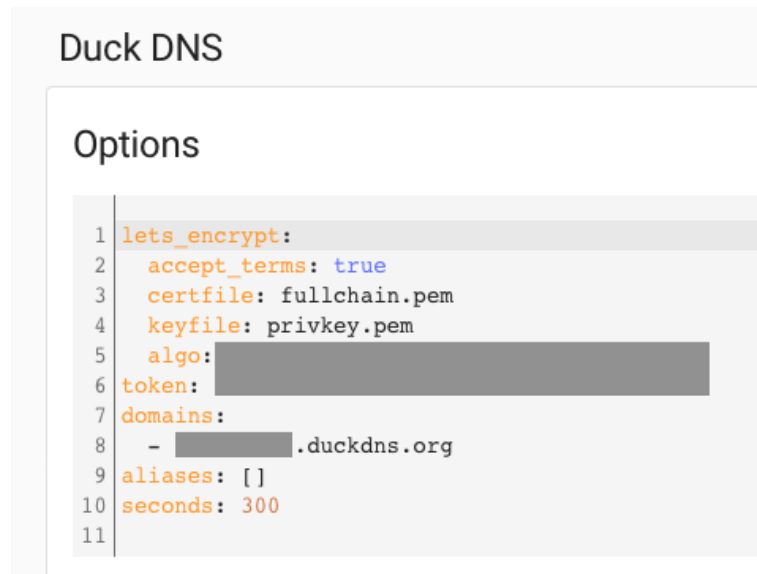
Käytön helpottamista varten haluttiin hyödyntää myös dynaamista nimipalvelinta. Tämän avulla verkkosivun osoite on mahdollista muuttaa hankalasti muistettavista numerosarjoista helpommin muistettaviksi kirjaimiksi. Verkkosivulle siirryttäessä ihmiset käyttävät kirjoitettavia osoitteita, eivätkä numeerisia IP-osoitteita. Tämä helpottaa suuresti sivuston käyttöä esimerkiksi seuraavilla tavoilla. Ensimmäiseksi, sivuston osoitteen muistaminen helpottuu merkittävästi, koska se on mahdollista muuntaa selkokielisemmäksi versioksi numerosarjan asemasta. Toiseksi, dynaaminen nimipalvelin pitää huolen siitä, että mikäli sivuston IP-osoite muuttuisikin, niin käyttäjä ei tätä huomaisi käytössä. Tällöin sivusto ohjautuu aina automaattisesti oikeaan IP-osoitteeseen.

Ryhdyttiin etsimään palvelua, joka toteuttaisi tämän vaatimuksen asennukselle. Saatavilla oli useita erilaisia ilmaisia vaihtoehtoja, kuten ClouDNS, Dynu ja Duck DNS [46]. Lopulta päädyttiin ottamaan käyttöön Duck DNS useiden internetistä löytyneiden suositusten perusteella. Home Assistantissa on tälle suora natiivituki lisäosan muodossa. Palvelun käyttö on mahdollista esimerkiksi oman Github-tilin avulla. Palvelu tarjoaa ilmaiseksi useiden eri osoitteiden käyttämisen DNS-palvelussa. Päädyttiin lopulta käyttämään kahta eri osoitetta: ensimmäinen osoite on Home Assistantille ja toinen OpenVPN:lle. Jokainen Duck DNS -palvelusta käytettävä osoite päättyy aina ”.duckdns.org”. Käyttäjällä ei siis itse voi määrittää kokonaista osoitetta, vaan pystyy vaikuttamaan vain sen alkuosaan.

Palvelu tarkistaa aina määräajoin palvelimelta IP-osoitteen ja havaitsee mahdolliset muutokset erittäin nopeasti. Käyttäjällä ei siis tarvitse huolehtia osoitteiden muutoksista, etenkin mobiiliverkkoa käyttävissä asennuksissa, joissa IP-osoitteet saattavat vaihdella useasti.

Duck DNS saadaan käyttöön asentamalla se Home Assistantin lisäosista. Ennen lisäosan käynnistämistä tulee Duck DNS:n verkkosivulta noutaa *token* ja samalla päättää haluttu verkkotunnus. Kirjautuminen onnistuu esimerkiksi Githubin tai Googlen kautta. Kun kirjautuminen on suoritettu ja saadut tiedot ovat tallella, asetetaan ne lisäosan Config-

sivulla oleviin kenttiin, kuten kuvassa 3.7. Lisäksi kohta "accept_terms" tulee muuttaa *falsen* asemesta *trueksi*. Tällöin käyttäjä hyväksyy käyttöehdot. Lopuksi lisäosa tulee käynnistää. Lisätietoja on saatavilla dokumentaationsivulta [47].



Kuva 3.7: Duck DNS -lisäosan asetussivu, josta piilotettu algo, token ja domain

Tämän lisäksi Home Assistantin omasta config-tiedostosta on määritettävä käyttöön Duck DNS ja sen tarjoama TSL-salausprotokolla kuten kuvassa 3.8 on esitelty. Tämä hyödyntää varmenteita yhteyksien suojaamisessa. Kirjoittaminen config-tiedostoon tapahtuu YAML-kielellä, joka vaatii huolellisen kirjoitusasun mm. välimerkit ja sisennykset.

Muutetut asetukset tulee tallentaa ja järjestelmä käynnistää uudelleen asetuksista, jotta muutokset astuvat voimaan. Tämän jälkeen järjestelmään pääsee kirjautumaan kuvan 3.9 mukaisesti aiemmin määritellystä osoitteesta.

```
/config/configuration.yaml
85
86 http:
87   · base_url: https://[redacted].duckdns.org:8123
88   · ssl_certificate: /ssl/fullchain.pem
89   · ssl_key: /ssl/privkey.pem
90   · ip_ban_enabled: true
91   · login_attempts_threshold: 5
92
```

Kuva 3.8: Home Assistantin config-tiedoston muokkaus. (Kuvassa SSL, vaikka oikeasti tarkoittaa TLS)



Home Assistant

Olet antamassa pääsyn <https://192.168.1.115:8123/> Home Assistant -ympäristöösi.

Kirjaudutaan sisään **Home Assistant Local**.



☐ Pidä minut kirjautuneena sisään

KIRJAUDU SISÄÄN

Kuva 3.9: Järjestelmän kirjautumissivu, paikallisesta osoitteesta

Luku 4

Järjestelmän määrittely ja toteutus

4.1 Käyttöliittymät

Käytettäväksi älykotialustaksi valikoitui Home Assistant, koska siitä oli runsaasti dokumentaatiota, useita opetusvideoita ja aktiivinen käyttäjäyhteisö. Päivityksiä julkaistaan viikoittain ja uusia ominaisuuksia ja laitteita lisätään tuetuiksi jatkuvasti.

Heti aluksi haluttiin toteuttaa Home Assistanttiin käyttöliittymät tietokoneelle, älypuhelimelle ja tabletille. Home Assistantissa tämä on mahdollista toteuttaa *dashboardien*, eli graafisten käyttöliittymien avulla. Lisädokumentaatiota on saatavilla internetsivulta [48]. Kyseisiä näkymiä on mahdollista muokata sopivaksi jokaiseen käyttötarkoitukseen sijoittamalla ”kortteja” haluttuun paikkaan ja valitsemalla haluttu tieto näytettäväksi. On esimerkiksi mahdollista tehdä lämpötilakortti, joka näyttää mittarina kodista löytyvän lämpötila-anturin mittaustuloksia reaaliajassa. Oleellista käyttöliittymäsuunnittelussa on tunnistaa käytettävän laitteen erityisominaisuudet, kuten kosketuksella ohjaaminen ja erilaiset käytettävien näyttöjen koot.

4.2 Järjestelmän määrittely

Projekti aloitettiin hyödyntämällä Raspberry Pi 3 Model B+ -yhden piirilevyn tietokonetta [24], SSD-kovalevyä ja Zigbee USB-tikkua. Järjestelmästä saatiin suhteellisen vakaa. Laitteisto toimi aluksi hyvin, mutta päivitysten ja lisääntyneiden integraatioiden myötä havaittiin järjestelmän olevan hieman alitehoinen kaikkien toimintojen ylläpitoon. Jatkuvan päivitystarpeen ja uudelleenkäynnistysten ajoittaisten ongelmien takia päädyttiin kuitenkin käyttämään Lenovon Thinkcentre Tiny -tietokonetta [49]. Pääsyy valinnalle oli koneen erittäin kompakti koko ja vähäinen virrankulutus. Suositeltu tapa asentaa Home Assistant olisi ollut asentaa käyttöjärjestelmä suoraan tietokoneen kovalevylle. Tietokoneessa oli kuitenkin merkittävästi enemmän suorituskykyä, muistia ja kovalevytilaa, kuin järjestelmä vaatii toimiakseen. Näistä seikoista johtuen tietokoneeseen päädyttiin asentamaan virtuaalikonealusta, jonka avulla yhdellä tietokoneella voi käyttää samanaikaisesti useita käyttöjärjestelmiä omina virtuaalikoneinaan. Laitteisto päädyttiin sijoittamaan kuvan 4.1 mukaisesti TV-tason sisälle.

Tietokoneen ominaisuudet:

- Malli: Lenovo Thinkcentre M600
- Prosessori: Intel Pentium N3700, 4-ytiminen, 1.60 GHz
- RAM-muisti: 8GB
- Kovalevy: 128GB SSD

Aluksi tietokoneeseen yritettiin asentaa tunnettua ja suosittua tyypin 1 VMware ESXi -virtuaalikonealustaa, jonka käyttö oli tutkielman kirjoittajalle tullut tutuksi työelämästä. Tyypin 1, natiivi, virtuaalikonealusta tarkoittaa sitä, että se toimii suoraan isännän raudan päällä [50, 51]. Kyseinen virtuaalikonealusta on kuitenkin paljon tarkempi toimimiseen vaatimistaan komponenteista. Kyseinen tietokone ei ollut tuettujen laitteiden luettelossa [52]. Useiden epäonnistuneiden asennusyritysten jälkeen VMwaren asentamises-



Kuva 4.1: Kuva järjestelmän laitteiston toteutuksesta

ta luovuttiin ja alettiin etsiä korvaavaa vaihtoehtoa. Tilalle löytyi ilmainen, avoimeen lähdekoodiin perustuva Proxmox-virtuaalikonealusta [53]. Havaittiin ohjelmiston täyttävän samat halutut kriteerit virtuaalikoneiden hallinnoinnille, kuin VMwarenkin tuote.

Proxmoxin asennus tapahtui samaan tapaan kuin muidenkin käyttöjärjestelmien asennus; lataamalla asennustiedosto, kirjoittamalla se USB-tikulle ja kytkemällä USB-tikku palvelintietokoneeseen. BIOS:sta valittiin USB-tikku halutuksi ensimmäiseksi käynnistyslevyksi. Uudelleenkäynnistyksen jälkeen tietokone avasi Proxmoxin asennusvelhon, jonka avulla asennus onnistui helposti ohjeita seuraten.

4.3 Yleiset älykotien kommunikaatioteknologiat

4.3.1 Langaton lähiverkko, Wi-Fi

Langaton lähiverkko, Wi-Fi (engl. Wireless Fidelity), tarkoittaa yleistä, kodeissa käytettävää langatonta verkkoteknologiaa. Tämä mahdollistaa laitteiden kommunikoinnin internetiin langattomasti. Tämä on erittäin yleinen tapa yhdistää laitteita internetiin ja se onkin tästä syystä käytössä niin toimistoissa, kodeissa, kahviloissa kuin hotelleissakin. [29]

4.3.2 Zigbee

Zigbee on teknologia, joka sai nimensä siitä, miten ampiaiset ”zig-zagaavat” kukkien välillä ja kertovat toisilleen informaatiota. Se on standardi, joka keskittyy tekniikan standardointiin ja laitteiden keskittaiseen toimivuuteen. Zigbee-laitteet eivät vaadi suurta kaistanleveyttä toimiaakseen, mutta alhainen latenssi ja pitkä paristojen käyttöikä ovat vaadittuja ominaisuuksia. Se onkin periaatteeltaan verrattavissa Bluetoothiin, mutta eroaa siitä esimerkiksi siten, että laitteet niin sanotusti nukkuvat enemmän ja käyttävät siitä johtuen vähemmän virtaa. [54]

Suuri ero Zigbee-verkossa verrattuna muihin tekniikoihin on sen kolme eri topologiaa. Nämä ovat tähti-, puu- ja mesh -topologiat. Laitteita näissä topologioissa on koordinaattori sekä reitittimet ja päätelaitteet. Yhdessä verkossa on aina tasan yksi koordinaattori. Tähtitopologia on näistä yksinkertaisin, sillä se muodostuu vain suoraan koordinaattorille kommunikoivista päätelaitteista. Puutopologiassa päätelaitteet kommunikoivat koordinaattorille pääosin reitittimien kautta. Mesh-topologia on näistä monimutkaisin, sillä siinä kaikki laitteet voivat keskustella toistensa kautta. Etuna Zigbeessä on se, että kukin reititin pidentää verkon kantavuutta ja voimakkuutta. [54, 55]

4.3.3 Bluetooth

Bluetooth on radioteknologia, jonka kantamaa voidaan pitää lyhyenä ja virrankulutusta vähäisenä. Varsinkin nykypäivänä yleinen Bluetooth LE (engl. low energy) on erittäin vähän virtaa kuluttava standardi. Tämä tekniikka on ollut käytössä yleisimmin esimerkiksi matkapuhelimeissa, tietokoneissa ja erilaisissa näiden lisälaitteissa, kuten kuulokkeissa. [56] Taulukossa 4.1 on vertailtu tekniikoiden välisiä eroja.

Standardi:	Wi-Fi	Zigbee	Bluetooth
Kantama (m):	1-100	1-75+	1-10+
Patterin kesto (pv):	0,1-5	100-1000+	1-7

Taulukko 4.1: Taulukko eri IoT-teknologioiden eroavaisuuksista [54]

4.4 Valmiit laitteet ja niiden integrointi järjestelmään

4.4.1 Philips Hue -älyvalot

Valaistus on olennainen osa kodissa, joten oli tärkeää saada se toimimaan älykkäästi järjestelmän avulla. Valaistuksen ohjaus toteutettiin niin, että ohjaaminen onnistuisi kahdella tavalla – joko Philipsin oman sovelluksen tai Home Assistantin kautta. Näin haluttiin varmistaa järjestelmän toimivuus, mikäli Home Assistant jostain syystä lakkaisi toimimasta.

Älyvalojen [5] ensimmäinen käyttöönotto tehtiin täysin valmistajan ohjeiden mukaan lisäämällä valoja Philips Huen siltaan. Tämä aloitettiin luomalla Philips-tili, jonka avulla valojen etäohjaus asunnon ulkopuolelta tuli myös mahdolliseksi. Tämän jälkeen silta kytkettiin kaapelilla verkkoon ja avattiin Hue-sovellus ja lisättiin valot sovellukseen. Käyttöönotto oli erittäin sujuvaa ja vaivatonta. Samalla tavalla tapahtui myös liikeseenso-reiden ja valokatkaisijoiden lisääminen.

Hue-valojen lisääminen Home Assistantiin onnistui integraation avulla, eli järjestelmään syötettiin vain oma käyttäjätunnus ja salasana. Tämän jälkeen tiedot synkronoituivat järjestelmään kuvan 4.2 mukaisesti suoraan Philipsin palvelimien kautta.



Kuva 4.2: Philips Hue integroituna järjestelmään

Philipsin älyvalojärjestelmä tukee nykyään myös Lidl Silvercrest -älykotijärjestelmän valaisimia ja katkaisijoita. Tätä haluttiinkin kokeilla Lidlin älypistorasian lisäämisellä järjestelmään ja nopeasti todettiin tämä täysin toimivaksi. Laitteen paritus siltaan tapahtui samalla tavalla kuin Philipsin omienkin laitteiden kanssa ja toimintavarmuuskin vaikutti olevan samalla, korkealla tasolla. Laite on ollut todella toimintavarma ja vakaa. Sitä ei ole myöskään tarvinnut parittaa uudelleen kertaakaan.

4.4.2 Amazon Alexa -älykotiapuri

Alettiin tutkia mahdollisen älykotiavustajan integroimista älykotijärjestelmään. Selvitystyön tuloksena päädyttiin valitsemaan älykotiavustajaksi Amazon Alexan sisältävä Echo Dot -laite. Toimintojen laajuus ja laitteen hankkimisen mahdollisuus olivat osaltaan määritteleviä syitä kyseiseen tuotteeseen päättymiselle. Laitteen ohjaaminen tapahtuu englannin kielellä, mikä tulee ottaa huomioon mahdollisia käyttökohteita harkittaessa.

Laite otettiin käyttöön normaalia asennusprosessia noudattaen. Älypuhelimeen ladattiin Alexa-sovellus ja tämän jälkeen asennus eteni ohjeita noudattaen eteenpäin. Laite kyt-

kettiin kotiverkkoon Wi-Fi:n avulla ja laitteiden integrointi Alexaan tapahtui automaattisesti kotiverkon skannauksen avulla. Sovellus kysyi mikä laite ja valmistaja halutaan löytää ja etsinnän jälkeen laite ilmestyi sovelluksen listaan. Alexa löysi hyvin laitteet kotiverkosta.

Alexan integrointi Home Assistanttiin oli haasteellisempaa. Alun perin tavoite ääniohjaukselle oli päästä ohjaamaan valaistusta ja muutamia Wi-Fi:n kytkettyjä laitteita. Projektin edetessä haluttiin myös selvittää olisiko mahdollista saada ääni-ilmoituksia Home Assistanttiin kytketyistä laitteista, kuten ovisensoreista ja tärinäsensoreista. Zigbee-tärinäsensori oli pitkän selvitystyön jälkeen mahdollista saada ilmoittamaan saapuneesta postista Alexan avulla, kuva 4.3. Tämä oli erittäin vaivalloinen prosessi, mutta lopulta kuitenkin mahdollinen.

Käytännössä tässä automaatiossa tarkkaillaan ovesta olevaan postiluukkuun kiinnitettyä tärinäanturia ja eteisen liiketunnistinta. Liiketunnistin on myös lisätty samaan automaatioon, jotta voitaisiin välttyä turhilta hälytyksiltä ihmisten liikkuesssa ulko-ovesta. Kun anturit havaitsevat minuutin sisällä vain tärinää eivätkä liikettä, järjestelmä lähettää tekstinä hälytyksen älypuhelimien ilmoituspalvelun kautta. Tämän lisäksi Amazon Alexa kertoo äänellä postin saapumisesta kaiuttimen välityksellä.

Posti hälytys tärinä



Kuva 4.3: YAML-koodi postihälytyksen automaatiosta

4.4.3 Zigbee-laitteet

Projekti aloitettiin sillä tavoitteella, että mahdollisimman moni laite kytkeytyisi langattomasti Wi-Fi:n kautta älykotijärjestelmään. Tutkielman edetessä huomattiin kuitenkin nopeasti, että kerrostalossa ongelmaksi muodostui signaalin häiriöt. Nämä johtuivat langattomien laitteiden suuresta määrästä pienellä alueella.

Toiseksi ongelmaksi pelättiin muodostuvan langattoman verkon laitteiston toimintakyky. Langattomien laitteiden lisääntyessä tulisi langattoman verkon kuormitus kasvamaan. Tämän johdosta aloitettiin selvitys langattomien ja myös paristokäyttöisten laitteiden integroimiseksi älykotijärjestelmään. Tutkielman kirjoittajalle jo tutuksi tullut Philips Hue -järjestelmä oli vakuuttanut toimintavarmuudellaan ja käytettävyydellään. Edellä mainituista syistä johtuen selvitettiin myös toisen Zigbee-verkon pystyttämisen mahdollisuutta asuntoon.

Zigbee-verkon luomista tutkittiin ja lopulta löydettiin tieto, että verkon luominen generisellä Zigbee USB-tikulla olisi mahdollista. Verkkoa varten tilattiin Texas Instrumentsin Zigbee USB-tikku. Kyseinen laite toimitettiin ilman käyttämiseen vaadittua ohjelmistoa ja siihen jouduttiin ohjelmoimaan Raspberry Pi -tietokoneen pinnien avulla zigbee2mqtt-ohjelmisto. Tämän avulla tikun hyödyntäminen tuli mahdolliseksi. Ohjelmiston asennus vaati Raspberry Pi -tietokoneen käyttöä Linux-käyttöjärjestelmällä. Seuraavassa on käsitelty asennusprosessi askeleittain.

Tarvittavat laitteet ohjelmointia varten:

- Raspberry Pi -tietokone
- Kolvi ja tinaa
- 4 jumpperikaapelia
- CC2531 USB-tikku

Johtojen kolvaaminen on välttämätöntä, koska pinnit ovat erikokoisia Rasperryssä ja

Zigbee USB-tikussa. Pinnit tulee kytkeä taulukon 4.2 mukaisesti toisiinsa jumpperikaapeilla. Kuvassa 4.4 asennusprosessi käynnissä.

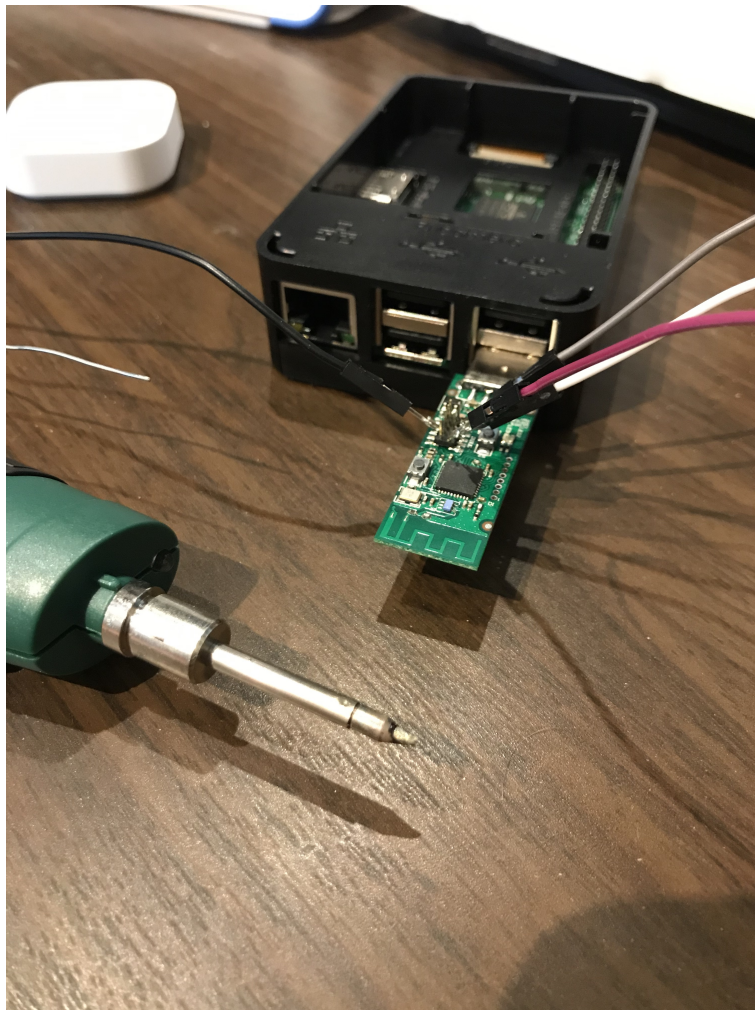
Raspberry Pi	CC2531
GND	GND
Pinni 38	DD
Pinni 36	DC
Pinni 35	RST

Taulukko 4.2: Tarvittavat kytkennät

Johtojen kytkemisen jälkeen käynnistettiin Raspberry Pi, johon oli asennettu Linux. Käytön helppouden vuoksi päädyttiin käyttämään Raspbian-versiota, ilman graafista käyttöliittymää. Ohjelmiston asennus tikulle tapahtui seuraavasti [57] :

1. Varmistetaan, että WiringPi on asennettuna komennolla: **sudo apt-get install wiringpi**
2. Kloonataan tikun ohjelmisto Raspberrylle: **git clone https://github.com/jmichault/flash_cc2531.git**
3. Siirrytään kansioon: **cd flash_cc2531**
4. Varmistetaan, että johdotus mennyt oikein: **./cc_chipid** Tulos pitäisi olla **ID = b524**
5. Ladataan zip-tiedosto ja siirrä se Raspberrylle, kirjaa ylös kansio. Osoite tiedoston lataamiselle: **https://github.com/Koenkk/Z-Stack-firmware/tree/master/coordinator**
6. Asennetaan Raspberrylle unzip-ohjelma: **sudo apt-get install unzip**
7. Puretaan zip-tiedosto: **unzip CC2531_DEFAULT_20201127.zip**

8. Tyhjennetään flash muisti: `./cc_erase`
9. Siirretään tiedosto Raspberyllä tikulle: `./cc_write/polku/CC2531ZNP-Prod.hex`
10. Asennus kestää muutaman minuutin, lopuksi irroitetaan johdot ja sammutetaan Raspberry.



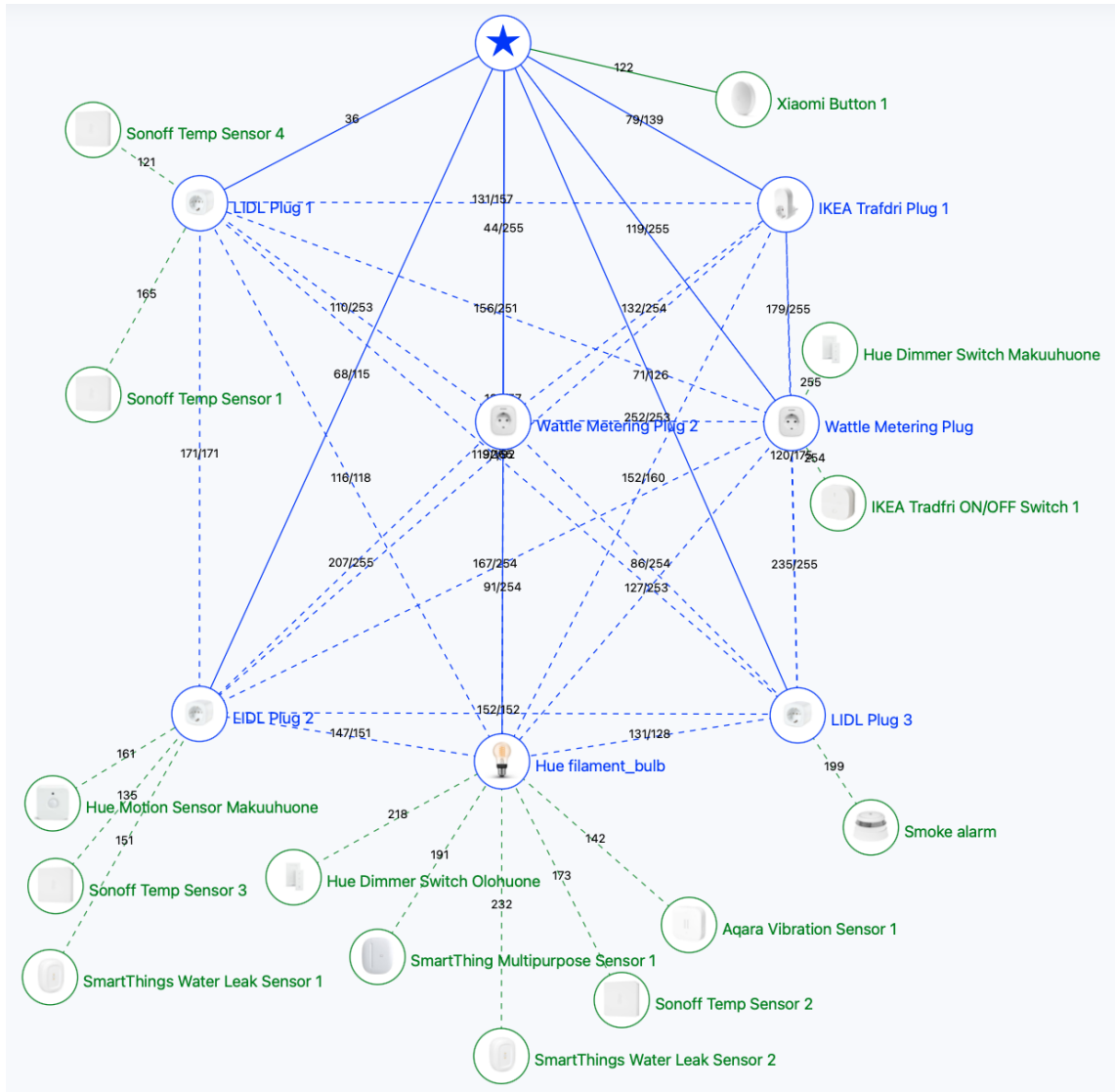
Kuva 4.4: Ohjelmiston asennus Zigbee USB-tikulle vaati kolvausta

Home Assistantiin tulee asentaa Zigbee Home Automation- tai zigbee2mqtt-ohjelmisto. Ohjelmiston avulla on mahdollista yhdistää erimerkkiset laitteet yhdeksi kokonaisuudeksi. Päädyttiin valitsemaan kuvan 4.5 zigbee2mqtt, jolla on laaja käyttäjäkunta ja josta on olemassa paljon dokumentaatiota.

Enter search criteria							
#	Pic	Friendly name	IEEE Address	Manufacturer	Model	LQI	Power
1		Sonoff Door Sensor	0x00124b001f906052 (0x47E8)	SONOFF	SNZB-04	N/A	
2		IKEA Tradfri ON/OFF Switch 1	0x5c0272fffe3c0fbe (0x800C)	IKEA	E1743	N/A	
3		Hue Dimmer Switch Olohuone	0x001788010637f9b5 (0xBDB0)	Philips	324131092621	N/A	4% 
4		Hue Motion Sensor Makuuhuone	0x0017880106f7e359 (0x2974)	Philips	9290012607	63	
5		LIDL Plug 1	0x842e14fffe6261d6 (0xD2D0)	Lidl	HG06337	63	
6		Hue filament_bulb	0x0017880108137213 (0x0764)	Philips	8718699688820	63	
7		Aqara Vibration Sensor 1	0x00158d0006d49040 (0xA90A)	Xiaomi	DJT11LM	N/A	

Kuva 4.5: Lista laitteista zigbee2mqtt-lisäosan sivulla

Home Assistantiin asennettu zigbee2mqtt-lisäosa piirtää kartan yhdistetyistä laitteista kuvassa 4.6.



Kuva 4.6: Zigbee2mqtt-lisäosan kuva laitekartasta

Järjestelmän laitteiden avulla haluttiin mitata ilmasta lämpötilaa ja ilmakeuhetta, oviantureilla tarkkailla ovien kiinnioloa, mittaavilla pistorasioilla tarkastella laitteiden virrankulutusta ja pistorasioiden avulla muuttaa tavallisia valoja älykkäiksi. Liikkeentunnistuksesta on tullut erittäin tärkeä osa älykotitoteutusta; se on mm. osoittautunut käteväksi tavaksi sytyttää valot eteisessä, kun saavutaan pimeään asuntoon. Tärkeä toiminto on myös sen toiminta osana murtohälytinja järjestelmää. Järjestelmän ollessa kytkettynä se lähettää ilmoituksen käyttäjän älypuhelimeen havaitusta liikkeestä.

Järjestelmässä käytettyjä Zigbee-laitteita listattuna:

1. Philips Hue: White and Color E27 -lamppuja, LightStrip-valonauhaa, liiketunnistimia, himmennyskytkimiä, Play Gradient -valonauhaa
2. Sonoff: SNZB-01 -painike, SNZB-02 -lämpötila- ja ilmakeuhesantureita, SNZB-03 -liiketunnistin ja SNZB-04 -ovimagneetteja
3. Xiaomi Mi: langaton painike
4. SmartThings: liiketunnistin, vesivuotohälytin ja monikäyttöinen sensori
5. Wattle: Connected Home Mini -palovaroitin, Smart-älypistorasia
6. Ikea: Trådfri langattomia himmentimiä ja älypistorasia
7. Aqara: Vibration Sensor -värinä- ja kallistustunnistin
8. Lidl: Älypistorasioita

4.4.4 Wi-Fi-laitteet

Langattomasti verkkoon kytkeytyviä Wi-Fi-laitteita tutkittiin projektin pohjatyötä tehdessä niiden käyttöönoton helppouden vuoksi. Laite pitäisi vain kytkeä internetiin ja yhdistää järjestelmään.

Tutkielman kirjoittaja oli ostanut jo ennen älykotiprojektin aloittamista verkkoon kytkeytyvän pistorasian ja valvontakameran. Pistorasia oli Energizer-merkkinen ja se toimi valmistajan oman pilven kautta ja sen ohjaus oli mahdollista myös ulkoverkosta. Ohjelmiston avulla oli myös mahdollista tehdä ajastuksia ja ajastimia rasian käyttöön. Valvontakamera oli Fujitech:n valmistama laite, joka toimi valmistajan oman pilven kautta. Pelkästään näiden kahden laitteen käyttöä varten oli pitänyt jo luoda kaksi eri käyttäjätiliä ja ladata puhelimeen kaksi eri sovellusta. Termi älykoti alkoi ajoittain tuntua kaukaisemalta, sovellusten määrän lisääntyessä jokaisen laitteen asennuksen jälkeen.

Paristokäyttöisten Wi-Fi-laitteiden mahdollisuuksia tutkittiin myös. Laitteita olisi saatavilla jonkin verran, mutta laitteiden pariston käyttöikä jäisi todella lyhyeksi verrattuna Zigbee-laitteisiin. Lisäksi laitteiden hinta oli noin 50 euroa, kun taas Zigbee-laitteita oli myynnissä alle 20 eurolla. Valmiiden Wi-Fi-laitteiden suuri etu olisi ollut niiden integroinnin helppous järjestelmään.

Internetin yli on mahdollista integroida dataa järjestelmään myös esimerkiksi mökiltä. Tämä toteutettiin rakentamalla mökille lämpötila-anturi, joka raportoi dataa avoimeen Thingspeak-palveluun [58]. Se on ilmainen tietokanta, jonne käyttäjien on mahdollista lähettää IoT-laitteidensa mittausarvoja. Sivuston tietokannasta integrointi Home Assistantiin oli helppoa ja sujuvaa. Tiivistetysti, koottu lämpötila-anturi lähettää mittausdatan pilvipalveluun, josta Home Assistant käy lukemassa arvoja ja ne voidaan tuoda esille halutulla tavalla. Tämä voidaan toteuttaa esimerkiksi historiakaavioiden avulla.

Home Assistantissa Wi-Fi-laitteiden viestintä toteutettiin MQTT:n avulla. Tämä on OASIS-standardin mukainen IoT-laitteiden viestintäprotokolla. Se on erittäin kevyt ja tehokas viestintäprotokolla, jonka avulla IoT-laitteiden viestintä on mahdollista. [59]

4.5 Itse koottujen laitteiden tekeminen älykotisopiviksi ja niiden integrointi

Tutkielman kirjoittaja halusi myös syventyä enemmän älykotilaitteiden kokoamiseen. Havaittiin, että kaikkiin haluttuihin älykotiratkaisuihin ei ollut olemassa valmista ratkaisua. Tämä pakotti tutkimisen laajentumaan myös tee se itse -laitteiden tekemisen mahdollisuuksiin.

4.5.1 Monivärinen LED-valonauha

Valmiita älykotiratkaisuja on nykyään todella moneen tarkoitukseen. Asunnossa, jonne älykotijärjestelmää oltiin toteuttamassa, oli olohuoneessa osittain madallettu katto. Tämän reunan havaittiin olevan tarpeeksi leveä LED-valonauhan kiinnitystä varten. Selvitystyö aloitettiin etsimällä valmiita ratkaisuja esimerkiksi Philips Hue:ta ja Osram Lightify:ta. Näiltä valmistajilta löytyi valmiita ratkaisuja, mutta laitteiden hinta ja käytön rajoittuneisuus muodostuivat ylitsepääsemättömiksi. Lopulta valaistus päädyttiin toteuttamaan itse tekemällä kuvan 4.7 mukaisesti. Käytetyt tarvikkeet listattuna:

- 5m RGB-ledivalonauhaa, IP30, 5V, 30 LED/m, WS2812BECO-tyyppi
- NodeMCU v3 IoT -mikrokontrolleri
- Virtalähde 5V LED-valoille
- Virtajohto ja jumpperikaapeleita
- Kolvi ja tinaa

Kyseiseen toteutukseen päädyttiin, kun tutkinnan tuloksena löydettiin WLED-niminen ohjelmisto [60], joka oli mahdollista ohjelmoida NodeMCU-mikrokontrollerille. Tämän ohjelmiston avulla valonauhan ohjaaminen on mahdollista yksittäisten ledien tarkkuudella. Siihen voidaan määrittää erilaisia efektejä koko valonauhan mitalta ilman, että efek-

ti on sama koko mitalta. Valonauha voi esimerkiksi aaltoilla sinivalkoisena vaihtelevalla nopeudella ja kirkkaudella. Lisäksi se on mahdollista ohjelmoida siten, että se reagoi auringon kiertoon.



Kuva 4.7: Lopullinen asennus toimivana kokonaisuutena

4.5.2 Lämpötilamittari

Keittiössä ikkunan ja kalusteiden sijainti mahdollisti sen, että voitiin mitata samalla anturilla sisä- ja ulkolämpötilaa. Ulkolämpötilan mittaamisen haaste oli siinä, että piti löytää anturi, joka ylittäisi tarpeeksi ulos tuuletusikkunasta. Käyttötarkoitukseen valikoitui DS18B20-anturi yhden metrin mittaisena. Kaapeli oli tarpeeksi ohut, jotta sen pystyi vetämään ulos ikkunan välistä. Kaapelin päässä olevan mitta-anturin sijoitus onnistui siis erittäin hyvin, koska se voitiin asentaa siten, että se on tarpeeksi kaukana ikkunasta sekä myös irti talon seinästä. Näin toimimalla saavutettiin mahdollisimman tarkat mitaustulokset. Anturi antaa mitaustulokset 0,1 asteen tarkkuudella, jonka todettiin olevan käyttötarkoitukseen riittävä.

Sisälämpötilan mittaamiseen vaadituksi anturiksi valikoitui DHT11-anturi. Kyseinen anturi oli ollut jo kauan markkinoilla ja siitä oli paljon positiivista palautetta tuotesivuilla. Tämä anturi mittaa lämpötilan lisäksi myös ilmentöteutta, se oli yhdenmukainen mui-

den asunnon Zigbee-antureiden kanssa, jotka myöskin mittasivat lämpötilan lisäksi ilmankosteutta. Kyseisen anturin todella huokea yhden euron hinta helpotti myös anturin valinnassa. Kuvassa 4.8 on valmis toteutus toimivasta laitteesta.

Antureiden mittaama tieto piti saada lähetettyä Home Assistantille. Tähän tehtävään valittiin pienen kokonsa takia WeMos D1 Mini -mikrokontrolleri. Tämä laite mahdollisti myös useiden anturien liittämisen, joten valinta oli helppo tehdä.

Käytetyt tarvikkeet:

- DHT11-lämpötila-anturi
- WeMos D1 Mini IoT -mikrokontrolleri (ESP8266)
- USB-virtalähde
- Micro-USB latauskaapeli
- Kolvi ja tinaa

Laitteeseen asennettiin Tasmota-ohjelmisto [61], jonka avulla datan tarkastelu ja välittäminen on mahdollista. Lisää tästä ohjelmistosta ja sen asennuksesta seuraavassa kappaleessa.



Kuva 4.8: Ulko- ja sisälämpötilaa mittaava anturi valmiina

4.5.3 Wi-Fi-älypistorasian modifiointi

Tutkielman kirjoittajan ensimmäisiä IoT-laitteita olivat marketista ostetut Wi-Fi-älypistorasiat. Niiden ohjaus tapahtui puhelinsovelluksella, valmistajan pilven kautta. Vaikka Home Assistant tukee suuren määrän eri valmistajien laitteiden integraatioita valmiina, näitä laitteita ei ollut tuettuina. Toisaalta tämä kääntyi nopeasti positiiviseksi asiaksi, sillä tutkimalla löydettiin tieto, että älypistorasian ESP-piirilevylle olisi mahdollista ohjelmoida avoimeen lähdekoodiin perustuva Tasmota-ohjelmisto [61]. Sen avulla älypistorasiat saadaan toimimaan vain paikallisesti, ilman tarvetta valmistajan pilvipalvelulle. Laitteiden kyberturvallisuus paranee tästä johtuen erittäin paljon, koska pistorasiat eivät enää vaadi jatkuvaa yhteyttä internetiin.

Ohjelmointiin tarvittiin:

- Tietokone ohjelmointia varten (Linux, Windows tai MacOS)
- Serial-to-USB-adapteri
- Micro-USB-latauskaapeli
- Kolvi ja tinaa
- Jumpperikaapeleita
- Älypistorasia ohjelmoitavaksi

Ohjelmoitava ESP-laite, älypistorasia, täytyy kytkeä USB-adapteriin taulukon 4.3 mukaisella tavalla. Kun laite yhdistetään tietokoneeseen, on laitteen painiketta pidettävä painettuna, jotta laite saadaan asetettua ohjelmointitilaan. Tutkielman kirjoitushetkellä helppoin ja toimivin tapa ohjelmoida Tasmota-ohjelmisto laitteeseen on käyttää web-asennusta [62] Chrome-selaimella. ESP32-pohjautuvan mikrokontrollerin asennus tapahtuu vielä helpommin, kytkemällä laite USB-kaapelilla tietokoneeseen ja asentamalla ohjelmisto internetselaimella laitteeseen. Tämän jälkeen ohjelmoitu laite muodostaa Wi-Fi-

Serial adapteri	ESP-laite
3V3	3V3 tai VCC
TX	RX
RX	TX
GND	GND

Taulukko 4.3: ESP-laitteen ja USB-adapterin väliset kytkennät

verkon, johon yhdistämällä päästään täyttämään halutun kotiverkon tunnukset. Kommunikointia varten tulee asettaa vaaditut MQTT [59]-asetukset.

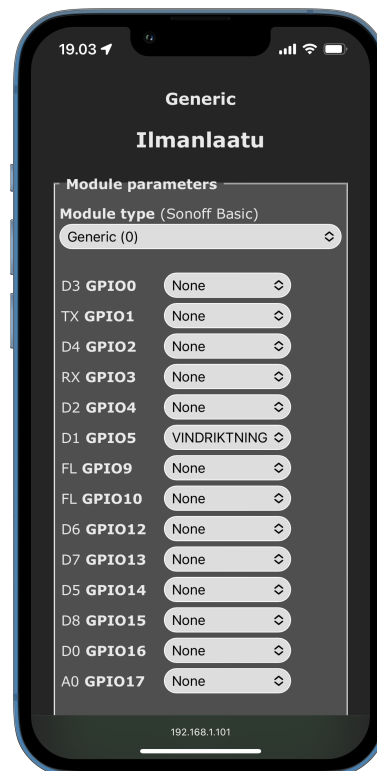
4.5.4 Ikean ilmanlaaduntunnistimen älyllistäminen

Ikea julkisti vuonna 2021 pienen ilmanlaaduntunnistimen, joka mittaa ilman pienhiukasia (PM_{2,5}) ja ilmoittaa saadut mittaustulokset laitteen kuvassa 4.11 näkyvien LED-valojen avulla ilmanlaadun kolmena eri tasona. Tämä oli harvinainen löydös, sillä hintaa laitteella oli vain reilut 10 euroa. Laitteen tietoihin tutustuttaessa löydettiin sivusto [63], jolla oli kuvattuna, miten laite olisi mahdollista yhdistää Home Assistantiin WeMos D1 Minin avulla. Tällöin mittaustuloksia olisi mahdollista seurata muualtakin, kuin vain laitteen etupaneelistä. Myös historiatietojen tarkastelu tulisi samalla mahdolliseksi. Tämä olisi mahdollista asentamalla Tasmota-ohjelmisto WeMos D1 Miniin. Ilmanlaaduntunnistin ja WeMos D1 Mini yhdistettiin toisiinsa jumpperikaapeleilla kolva-ten taulukon 4.4 mukaisesti. Kuvassa 4.9 laitteen asetuksista valittiin D1-pinniin haluttu Vindriktning-vaihtoehto.

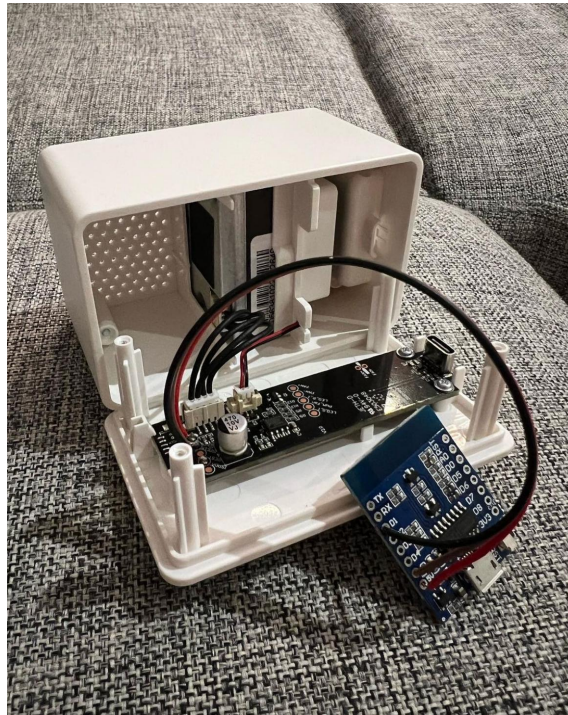
Tämän jälkeen Tasmotan asetuksiin täytettiin oikeat MQTT-tiedot ja sen jälkeen laite alkoi lähettää tietoja Home Assistantiin. Saavutettuna hyötynä tästä oli historiatietojen keruu, jolloin on helpompaa yhdistää tiettyjä muuttujia ilmanlaatuun vaikuttaviksi tekijöiksi. Yhtenä esimerkkinä havaittiin ruoanlaitto, jonka havaittiin vaikuttavan suoranaisesti ilmanlaadun mittaustuloksiin. Laite kytkettynä taulukon 4.4 mukaisesti kuvassa 4.10.

Vindriktning	ESP-laite
5V	5V
REST	D1
GND	GND

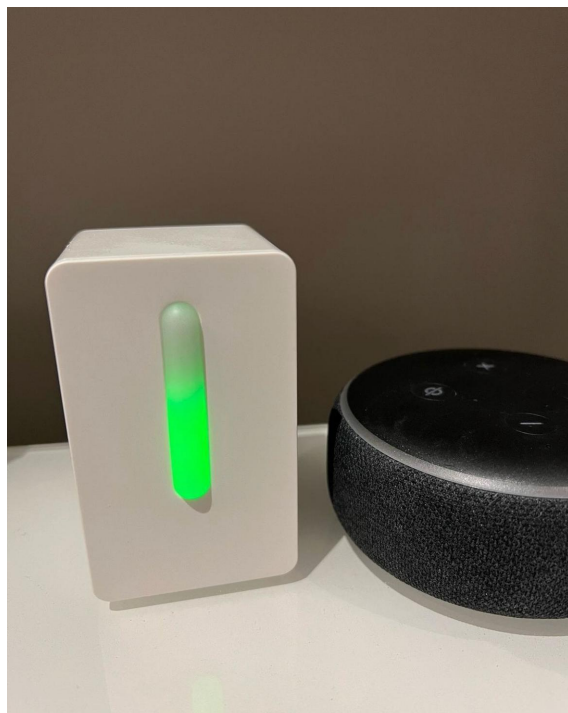
Taulukko 4.4: Vindriktning-ilmanlaaduntunnistimen ja WeMos D1 Minin väliset kytkennät



Kuva 4.9: Tasmotan hallintasivu ilmanlaaduntunnistimelle



Kuva 4.10: Ilmanlaaduntunnistin avattuna ja kytkennät tehtyinä

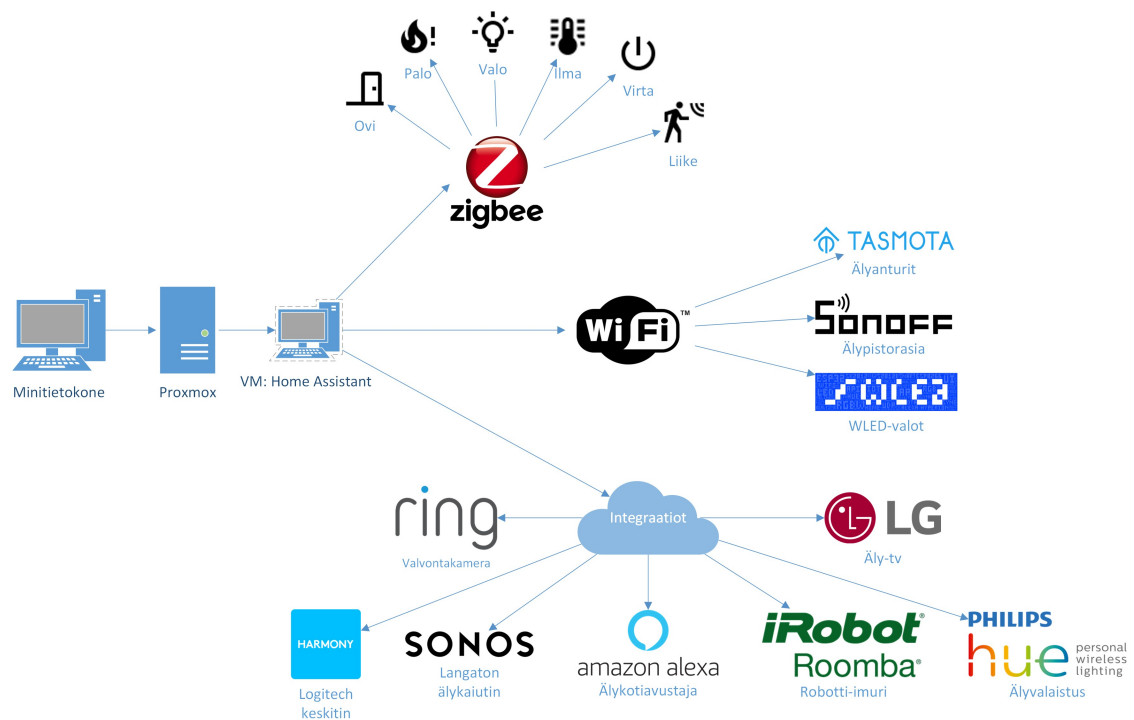


Kuva 4.11: Ilmanlaaduntunnistimen etupaneelin valot indikoimassa hyvää ilmanlaatua

4.6 Älykotiarkkitehtuuri

Älykotiprojekti laajeni työn edetessä paljon. Lopulta laitteistossa oli pelkästään jo erilaisia Zigbee-laitteita neljäkymmentä kappaletta.

Kuvassa 4.12 esitellään järjestelmässä olevia laitteita. Eriteltynä on järjestelmäintegraation avulla saavutettu käytettävyys – valmistajan pilvipalvelusta riippuva laitteisto. Omana osionaan esitetään Zigbee-laitteisto.



Kuva 4.12: Kaavio toteutuneesta laitteistosta

4.6.1 Laitteiden toiminnan haittoina riippuvuus pilvipalvelusta

Tutkielman aiheeseen vahvasti liittyen löytyi tieto, että Osramin Lightifyn palvelimet sammutettiin elokuussa vuonna 2021 [64] melkein seitsemän vuoden jälkeen aloitukselta. Tämän johdosta älyvalojen etäkäyttö kodin ulkopuolelta on muuttunut mahdottomaksi virallisen sovelluksen avulla. Lisäksi ääniavustajien (Alexa, Google) tuki on lopetettu. Tämä osoittaaakin hyvin, miksi pilvipalveluriippuvuudesta olisi toivottavaa päästä eroon.

Moni Lightify-käyttäjä joutuu nyt pohtimaan miten saa valonsa toimimaan edelleen haluamallaan tavalla. Havaitaan, että oman älykotipalvelimen ylläpidolla on konkreettisia etuja. Koska laitteet kommunikoivat suoraan kotona olevalle palvelimelle, eikä internetin yli valmistajan pilvipalvelimille, laitteiden käytettävyys tulee varmistetuksi.

Toinen esimerkki, joka löydettiin laitteiston käyttöikään liittyvästä tuen päättymisestä, on Philips Huen ensimmäisen sukupolven silta. Tämän, vuonna 2012 vuonna julkaistun, ensimmäisen sukupolven sillan tuki päättyi huhtikuussa vuonna 2020 [65]. Valojen ohjaaminen on tosin edelleen mahdollista, mutta mm. päivitykset ja tuki älykotiapureille päättyivät tuolloin. Moni käyttäjä närkästyi tästä uutisesta, koska heidän oli käytännössä pakko ostaa uusi versio sillasta, jotta ostetut ominaisuudet jatkaisivat toimintaansa halutunlaisesti.

Luku 5

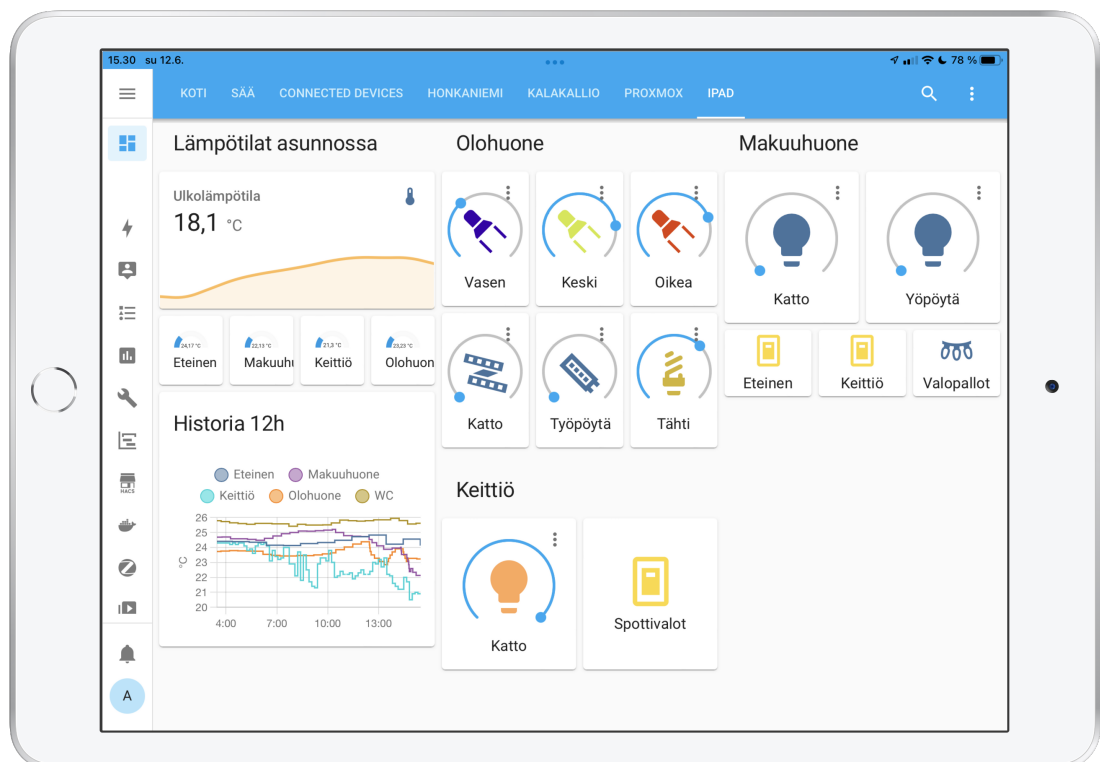
Testaus, havainnot ja pohdinta

Tuotetuen päättymisen on älykotilaitteisiin usein liittyvä ongelma. Kun kuluttaja ostaa laitteen, hän todennäköisesti kuvittelee laitteen toimivan kuvastusti koko laitteen käyttöiän ajan. Äkillinen tuen ja päivitysten päättymisen ajaa kuluttajan hankalaan tilanteeseen, kun laitteet eivät enää jatkakaan toimimista samalla tavalla. Hyvä etu Home Assistantissa onkin juuri laitteiden käyttöiän pidentäminen, sillä riippuvuus muista palveluista on mahdollista poistaa. Useat erimerkkiset älyvalot on mahdollista liittää myös Home Assistantin omaan Zigbee-reitittimeen ilman muita sovelluksia. Tämän kautta valojen ohjaaminen on silti mahdollista, vaikka valmistaja ei enää antaisikaan tuotetukea aiemmin hankituille valaisimille.

Järjestelmää on testattu jatkuvasti tutkielman kirjoittamisen ohessa. Jokaisen muutoksen ja laitteen lisäämisen jälkeen on varmistuttu siitä, että kyseinen laite toimii odotetusti ja varmasti. Mahdolliset automaatiot on luotu aina siten, että ne ovat toimivia ja toimintavarmoja. Eniten haasteita automaatioiden tekemisessä on aiheuttanut logiikan keksiminen. Välillä oli haastavaa hahmottaa myös automaation eteneminen. Tästä esimerkkinä eteisen postiluukkuun toteutettu tärinään reagoiva automaatio, joka ilmoittaa käyttäjälle saapuneesta postista. Tässä olivat haasteena aluksi turhat hälytykset. Nämä saatiin kuitenkin häviämään ottamalla automaatioon mukaan eteisessä sijaitseva liiketunnistin. Tämän tunnistimen avulla oli mahdollista määritellä tärinäanturi antamaan hälytyksiä vain sil-

loin, kun eteisessä ei havaita liikettä minuutin sisällä tärinän havaitsemisesta. Tällöin on varmaa, ettei havaittu tärinä johdu asunnon ovesta kulkemisesta.

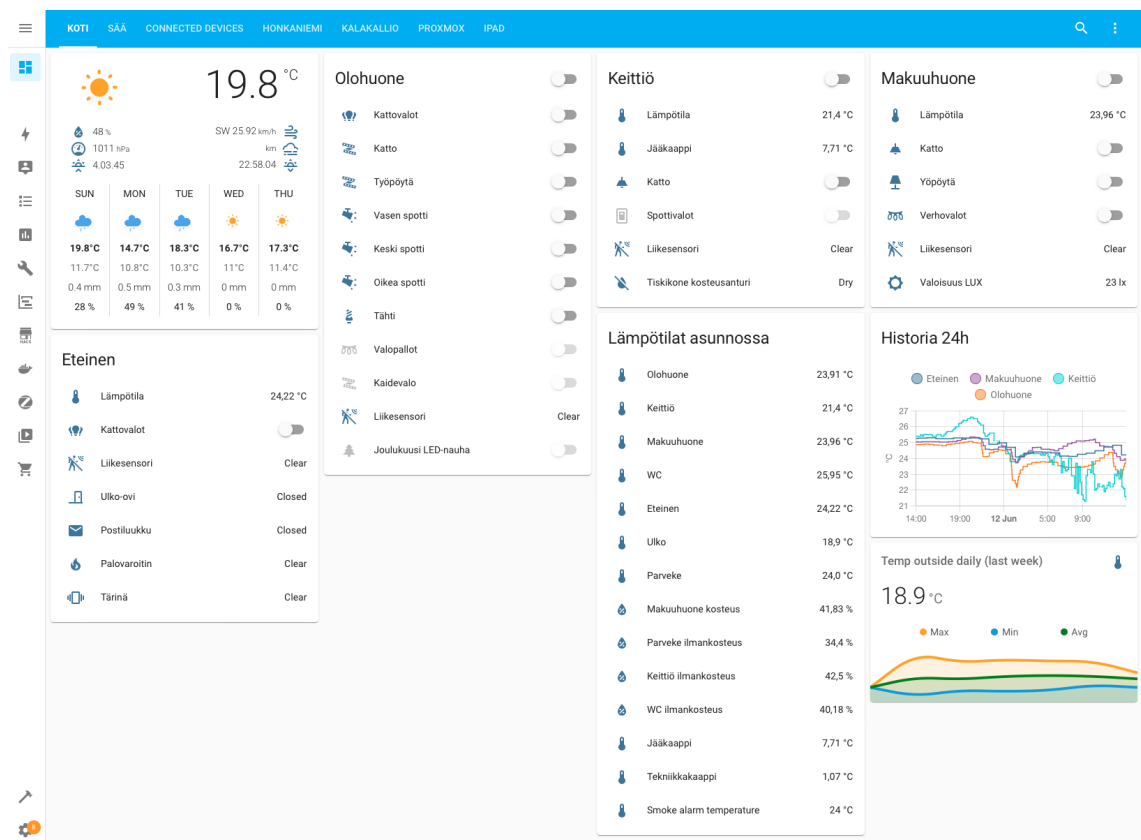
Järjestelmän käyttöliittymän parantelu vei useita viikkoja. Toimivimmiksi tavoiksi järjestelmän käyttämiselle todettiin olevan käyttö tietokoneen selaimen kautta ja älypuhelimien mobiilisovellus. Havaittiin nopeasti, että samanlainen käyttöliittymä ei toimi molemmissa tapauksissa. Mobiilikäyttö vaati täysin erilaisen käyttöliittymän toteuttamisen laitteen pienemmän näyttökoon sekä kosketuksella ohjaamisen takia. Verrattuna mobiilisovellukseen, järjestelmän käyttäminen tietokoneen selaimella mahdollistaa suuremman tietomäärän esittämisen käyttäjälle. Tulevaisuuden varalle toteutettiin kuvassa 5.1 näkyvä valmis käyttöliittymäsivu tabletin käyttöä varten. Tavoitteena olisi joskus toteuttaa asunnon eteiseen kiinteästi asennettu tabletti, jolta järjestelmän ohjaaminen ja monitorointi olisi mahdollista.



Kuva 5.1: Järjestelmän aloitussivu tabletilla

Tabletin käyttöliittymä suunniteltiin pelkistetyksi. Näkyviin asetettiin kuvassa 5.1 näkyvät asunnon tärkeimmät lämpötilat ja valot. Valojen ohjaamista varten valittiin painike, jolla myös kirkkauden säätö olisi mahdollisimman helppoa. Pitkään painamalla painiketta on myös mahdollista muuttaa Philips Hue -valojen väriä tai valkoisen valon sävyä.

Tutkielman edetessä havaittiin, että järjestelmän ohjaaminen tietokoneen kautta muuttui vähäiseksi, kun mobiilisovellus saatiin toimivaksi. Järjestelmän pääasialliseksi käytöksi tietokoneella muodostui järjestelmän konfigurointi ja muutosten tekeminen. Näiden toteuttaminen oli merkittävästi helpompaa tietokoneen käyttöliittymällä, kuin mobiilisovelluksilla. Tultiin siihen päätelmään, että selaimen kautta käytettävään näkymään voidaan huoletta asettaa näkyviin paljon tietoa, kuten kuvassa 5.2 näkyvä asunnon laitteiden kokonaiskuva.



Kuva 5.2: Järjestelmän aloitussivu selaimella

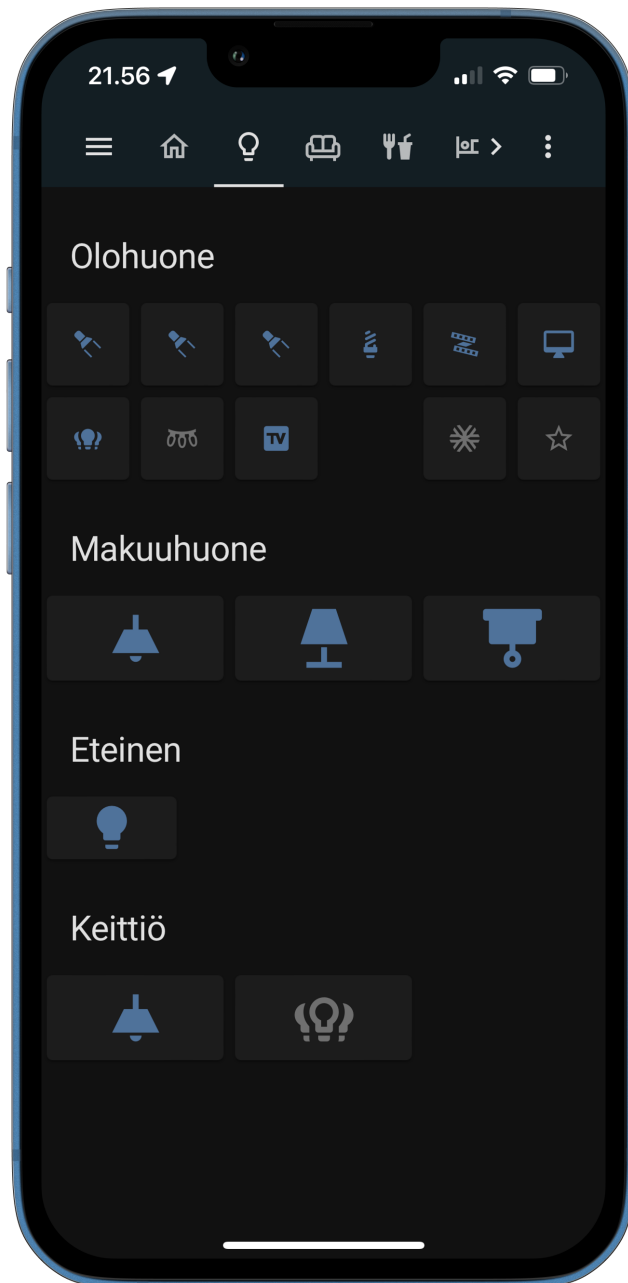
Matkapuhelimen pienempi näyttö asetti käyttöliittymän suunnittelulle haasteita. Väli-

lehtien vaihto suoritetaan ”karusellista”, jolloin navigointiriville on mahdollista sijoittaa enemmän sivuja. Nämä kuitenkin menevät piiloon käyttäjän selatessa sivua alaspäin. Sisältö tulisi priorisoida mobiilisuunnittelussa navigointipainikkeiden edelle [66]. Tämän vuoksi älypuhelinsovelluksen käyttöliittymässä on asetettu sivupalkki piiloon, koska siinä sijaitsevia painikkeita tarvitaan vain harvoin. Näihin on kuitenkin mahdollista päästä käsi vasemman yläkulman ”hampurilaisvalikon” kautta. Matkapuhelimen käyttöliittymään toteutettiin kuvassa 5.3 näkyvälle etusivulle valikoima tärkeimpiä tietoja asunnosta, säästä ja päiväkohtaiset nimipäiväsankarit. Asunnon tiedoista esitellään käyttäjälle palovaroittimen ja vesivuotosensorin tilat sekä tieto ulko-oven kiinnioloista. Sivulle on myös koodattu painike, jota painamalla asunnon jokainen valo sekä halutut pistorasiat sammuvat kertapainalluksella. Tämä sama toiminto on myös koodattu eteisessä olevaan Ikean Zigbee-painikkeeseen, mistä on tullut hyödyllinen ominaisuus asunnosta poistuttaessa. Aloitussivulla on myös kootusti tiedot asunnon lämpötiloista, ilmankosteuksista ja näiden 12 tunnin historiagraafit.

Mobiilinäkymän toiselle välilehdelle, kuvassa 5.4, on koottu näkyviin kaikki asunnon valot ja älypistorasiat. Sivun tarkoituksena on toimia selvänä visuaalisena sille, mitkä asunnon valoista ovat päällä. Seuraavaksi on luotu jokaiselle huoneelle oma sivunsa, jossa on kyseiseen huoneeseen liittyvää tietoa, kuten valot, lämpötilat, virrankulutukset ja Sonos-älykaiuttimet. Pelkästään lämpötiloille on kuvassa 5.5 omistettu oma sivunsa, josta on helposti nähtävissä koko asunnon tiedot.



Kuva 5.3: Järjestelmän aloitussivu älypuhelimella



Kuva 5.4: Valot kootusti yhdellä välilehdellä



Kuva 5.5: Asunnon lämpötilat esitetty mahdollisimman selkeästi

5.1 Miten kyberturvallisuutta voisi vielä parantaa?

Tässä tutkielmassa suunniteltiin ja toteutettiin kyberturvallinen ja toimiva älykotijärjestelmä. Kyberturvallisuutta pohdittiin monipuolisesti ja se saatiin toivotulle tasolle. Havaittiin kuitenkin, että kyberturvan edelleen lisääminen saattaisi vaikuttaa haitallisesti järjestelmän käyttömukavuuteen.

Turvallisuutta olisi mahdollista lisätä käyttämällä laitteistoa ilman internetiä. Tällöin käyttö onnistuisi vain kotiverkkoon kytketyn laitteen kautta. Seuraava askel tästä olisi laitteiston käyttäminen pelkästään langallisten laitteiden kautta, kuten esimerkiksi tietokoneen avulla. Tällöin minimoitaisiin myös ulkopuolisten laitteistoon käsiksi pääsemisen riski rajoittamalla sen toiminta vain langalliseen kotiverkkoon, joka voitaisiin erottaa täysin langattomasta verkosta. Huomataan nopeasti, että tämä tuskin olisi käyttäjäystävällinen lähestymistapa älykotijärjestelmän ohjaamiseen. Laitteiden ohjaaminen langattomilla laitteilla on kuitenkin nykyaikainen, haluttu toiminnallisuus.

Järjestelmään otettiin käyttöön kaksivaiheinen tunnistautuminen, joka parantaa pelkän käyttäjätunnuksen ja salasanan heikkoutta. Salasanan arvo sisäänkirjautumisessa heikkenee, koska sen lisäksi vaaditaan vielä pääsy kaksivaiheisen tunnistussovelluksen tuottamaan kertakäyttökoodiin.

Järjestelmän käyttäminen VPN-yhteyden kautta todettiin myös mahdolliseksi toteuttaa ja tulokset tästä esiteltiin aiemmin kappaleessa 3.7. Käytön hankaluus nousi kuitenkin esteeksi tilanteessa, jossa järjestelmästä haluttiin tuottaa käyttäjälle esimerkiksi push-ilmoituksia älypuhelimeen. Valvontakameroiden lisääminen järjestelmään olisi toimenpide, jonka jälkeen VPN:n tuoma lisäturvallisuus voisi tulla aiheelliseksi. Tällöin ilmoituksille voisi toteuttaa toisen toimitusmuodon, kuten jonkin viestimen kautta lähetetyt sanomat käyttäjän viestisovellukseen. Valvontakameroiden kyberturvallisuuden lisääminen, mikäli ne olisivat kuvaamassa esimerkiksi sisätiloja, olisi varmasti tavoittelun arvoista.

5.2 Laitteiden käyttötarkoituksia

Langattomia Zigbee-lämpömittareita sijoitettiin jokaiseen asunnon huoneeseen. Lisäksi yksi mittari sijoitettiin jääkaappiin, jotta voidaan varmistua sopivasta jääkaapin lämpötilasta. Tämän avulla luotiin automaatio, joka muistuttaa hälytyksellä mikäli havaitaan, että jääkaapin lämpötila on noussut esiasetetun kynnyksen yli. Kylpyhuoneeseen päädyttiin myös asettamaan yksi anturi, jotta huoneen kuivumista ja lattian lämmitystä olisi mahdollista tarkkailla anturin tuottaman datan perusteella.

Parvekkeelle sijoitettiin Tasmota-pohjainen anturi, joka on kytketty parvekkeella olevaan pistorasiaan. Tämä anturi mittaa lämpötilaa, ilmankosteutta sekä ilmanpainetta. Keittiöön mittauksia tekemään asetettiin kuvan 4.8 anturi, joka mittaa sisälämpötilan ja ilman kosteuden lisäksi myös ulkolämpötilaa. Ulkolämpöä mittaava anturi oli mahdollista vetää ikkunakarmin välistä ulkoilmaan.

Liiketunnistimia on asunnon jokaisessa huoneessa. Pää tarkoitus näille on valaistuksen ohjaaminen. Näiden sensoreiden avulla oli mahdollista luoda Home Assistantissa automaatio, jonka avulla valot syttyvät ja sammuvat automaattisesti havaitusta liikkeestä. Automaatioita kehitettiin tutkielman aikana käyttäjäystävällisemmiksi esimerkiksi kelonajan mukaan mukautuvan lampun värilämpötilan avulla. Käytännössä tämä tarkoittaa, että päivisin valot syttyvät kirkkaan valkoisina ja iltaisin himmeinä ja lämpimän sävyisinä. Liiketunnistimien havaintoja hyödynnetään myös murtohälytyksissä.

Asunnon oviin asennettiin ovimagneetit. Näiden avulla eteisen valot syttyvät heti, kun ovi aukeaa. Tutkielman alussa eteisen valaistuksen sytytys toteutettiin eteisen liiketunnistimen avulla, mutta liikkeen havaitsemisessa kesti hieman liian kauan. Ovimagneetin avulla valot syttyvät jo ennen välioven avaamista asuntoon tultaessa. Yksi ovimagneetti asennettiin asunnon postiluukkuun. Tämän pohjalta luotiin automaatio, joka ilmoittaa postin saapumisesta. Se ei kuitenkaan ollut anturina tarpeeksi tarkka, sillä esimerkiksi ohut kirje saattoi jäädä usein huomaamatta. Tästä johtuen ovimagneetti korvattiin tärinää mittaavalla anturilla, joka havaitsee pienenkin tärinän ja pystyy raportoimaan luotettavasti

saapuneesta postista. Kuvassa 4.3 on esitelty tarkemmin tämän automaation koodia.

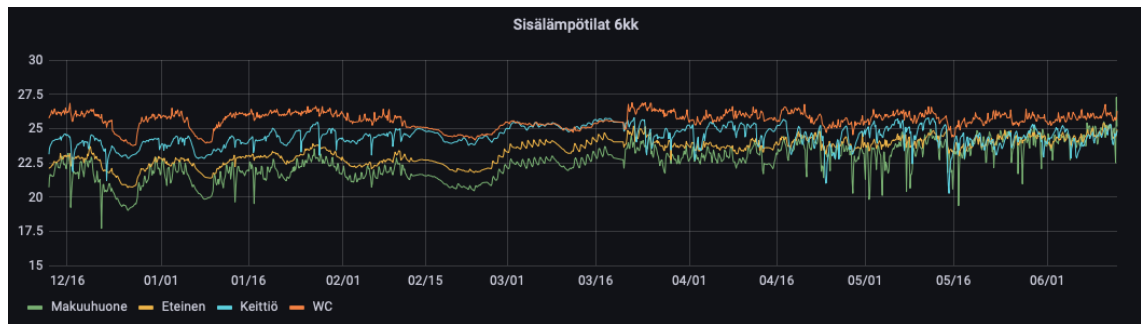
Älyvaloja on kylpyhuonetta lukuun ottamatta asunnon jokaisessa huoneessa. Valot ovat toimineet erittäin vakaasti. Osa asunnon valaistuksesta on toteutettu älypistorasioiden avulla, joihin on kytketty valaisimia. Laitteet on yhdistetty automaatioiden avulla yhtenäisiksi kokonaisuuksiksi. Esimerkiksi keittiössä Philips Hue -liikeanturi sytyttää Hue-älyvalon ja Tasmota-älypistorasian samanaikaisesti.

Langattomia painikkeita asetettiin jokaiseen huoneeseen, jotta valaistusta olisi mahdollista ohjata puheen ja älypuhelimien lisäksi myös niillä. Jokaiseen laitteeseen ohjelmoitiin erilaisia toimintoja erilaisille painalluksille. Esimerkiksi eteiseen sijoitettu päälle/pois painike sytyttää ja sammuttaa yhdellä painalluksella jokaisen asunnon valaisimen ja pistorasian. Tämä havaittiin käteväksi tavaksi varmistua asunnosta poistumisen yhteydessä siitä, että kaikki valot sammuvat.

5.3 Mitä havaittiin

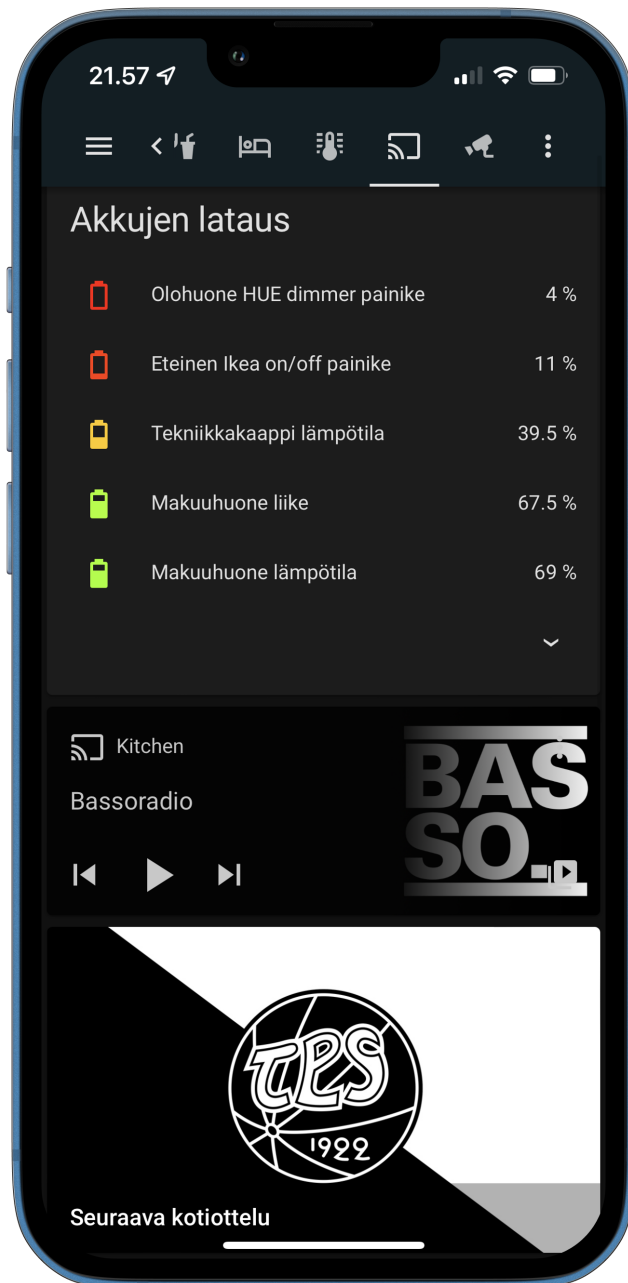
Eri valmistajien tekemien laitteiden yhdistäminen samaan älykotijärjestelmään todettiin mahdolliseksi. Valittu Home Assistant -alusta osoittautui erittäin monipuoliseksi ja toimivaksi. Sen avulla eri laitteiden yhdistäminen samaan käyttöliittymään oli mahdollista ja tuki erilaisille teknologioille oli saavutettavissa. Tutkielmassa toteutetun järjestelmän avulla mahdollistui esimerkiksi langatonta Zigbee-verkkoa hyödyntävän liiketunnistimen käyttö Wi-Fi-verkossa toimivan älyrasian ohjaamisessa. Tämä toteutettiin esimerkiksi keittiön kohdevalaisimissa. Järjestelmä saatiin toimimaan ja mittaustuloksiakin ehti kerrääntyä jo tutkielman tekemisen aikana runsaasti. Kuvasta 5.6 voidaan havaita, että järjestelmä saatiin toimimaan hyvin vakaana ja mittaustuloksiinkaan ei syntynyt aukkoja.

Mobiilikäyttöliittymään toteutettiin myös kuvan 5.5 mukainen välilehti, josta on helppo tarkastaa asunnon lämpötilat. Lisäksi valaistuksen käyttöä varten ohjelmoitiin kuvassa 5.4 näkyvä välilehti, joka helpottaa asunnon valaistuksen säätöä.



Kuva 5.6: Mittaustuloksia sisäilmasta kuuden kuukauden ajalta

Langattomia sensoreita varten luotiin käyttöliittymään kortti, joka hakee jokaisen laitteen senhetkisen pariston varauksen. Samaan aikaan laitteet järjestetään listaan siten, että ensimmäisenä listalla on heikoimman varauksen omaava sensori. Varauksen tilat esitetään kuvan 5.7 mukaisesti prosentteina, sekä havainnollistavana värinä: punainen tarkoittaa heikkoa varausta ja vihreä täyttä varausta.



Kuva 5.7: Langattomien laitteiden paristojen varaukset järjestyksessä

5.4 Ongelmat ja parannusideat

Tutkielmaa kirjoitettaessa havaittiin myös suuria eroja samankaltaisten laitteiden toiminnassa. Esille tulivat esimerkiksi erot Philips Hue ja Sonoff -liiketunnistimissa. Jälkimmäisen, niin sanottu cooldown-aika, eli se aika, jonka jälkeen laite pystyy taas havaitsemaan uudelleen liikettä, oli paljon pidempi kuin Philips Huen. Mikäli haluttiin saada valo syttymään liikkeestä vain 30 sekunniksi, todettiin Sonoffin anturi sopimattomaksi tähän tilanteeseen. Sen vaatima aika uuden liikkeen havaitsemiseksi mitattiin olevan 60 sekuntia. Philips Huen liiketunnistimella tämän ajan, tätä vastoin, mitattiin olevan vain 10 sekuntia. Tunnistin on tosin myös yli kolme kertaa kalliimpi kuin Sonoffin valmistama. Havaittiin, että laitteiden välillä on hinnan lisäksi myös muita, merkittäviäkin eroja ominaisuuksissa. Huen anturi pystyy esimerkiksi raportoimaan myös lämpötilan ja valon määrän.

Tutkielman tekemisen aikana tuli myös hyvin esille se seikka, että valmistajien tuki laitteille saattaa olla hyvinkin lyhyt. Aiemmin mainittiin esimerkiksi Osram Lightify -laitteiden tuen päättymisestä elokuussa vuonna 2021 [64]. Rakentamalla oma älykotijärjestelmä on mahdollista pidentää kalliiden laitteiden käyttöikää merkittävästi, ilman riippuvuutta laitteen valmistajan tuetusta.

Suoraan internetiin kytkettävien Wi-Fi-laitteiden tietoturva herättää suuria epäilyksiä. Projektin aikana testatuissa laitteissa päivityksiä ei tullut kertaakaan asennettavaksi, ja käytetty ohjelmisto saattoi olla jo vuosia vanha. Tällaisten laitteiden kytkeminen internetiin ei ole koskaan suositeltavaa niiden heikon tietoturvan vuoksi. Laitteiden päivittäminen voidaan jakaa karkeasti kahteen tapaan. Niiden päivitys voi tapahtua joko fyysisesti, esimerkiksi kytkemällä laite tietokoneeseen, tai OTA (engl. over-the-air) päivityksenä langattomasti laitteelle suoraan internetistä lataamalla.

Aiemmin tutkielmassa esitelty Tasmota-projekti helpottaa monella osa-alueella eri laitteiden tietoturvaa. Tämän ohjelmiston asentamisella laitteeseen saadaan siitä paikallisesti, vain kotiverkossa toimiva laite, kuten älypistorasia. Vaikka ohjelmiston asentaminen laitteeseen vaatii harrastuneisuutta, asennus voi laitekohtaisesti olla helppo tehtävä.

5.5 Ajankohtaiset mahdollisuudet energian säästämiseksi

Erittäin ajankohtaisiksi nousseita aiheita tutkielman kirjoittamisen aikana ovat energian säästäminen ja sähkönhinnan suuri nousu. Älykodin avulla toteutuu sähkön säästöä, esimerkiksi liiketunnistukseen perustuvan valaistuksen avulla valot eivät pala turhaan huoneissa. Lisäksi valaistus on mahdollista ajastaa syttymään vasta auringon laskettua illalla tai muuten olosuhteiden ollessa tarpeeksi pimeät. Näiden älykkäiden ominaisuuksien avulla saavutettu säästö sähkölaskussa on kuitenkin käytännössä suhteellisen pieni LED-valojen vähäisen virrankulutuksen vuoksi. Asia, jolla voitaisiin oikeasti vaikuttaa asuntojen sähkönkulutukseen on lämmityksen säätely ja optimointi. Tämä korostuu varsinkin talven kylminä kuukausina. Tällä hetkellä myynnissä olevista sähkösopimuksista suuri osa on pörssisähköön perustuvia. Näissä sähkön hinta heittelee ajoittain paljon päivän aikana. Älykkäällä lämmityksellä säästöä olisi mahdollista saavuttaa lämmityksen ohjauksella, joka perustuisi suoraan senhetkiseen sähkön hintaan. Esimerkiksi sähkön hinnan laskiessa arvon X alle, käynnistyisi ilmalämpöpumppu ja lämminvesivaraaja. Kun taas hinta nousisi arvon Y yli, sammuisivat nämä paljon sähköä kuluttavat laitteet pois päältä. Oleellista on kuitenkin ottaa huomioon myös ympäristön olosuhteet. Ei olisi optimaalista, että asuntoa ei lämmitettäisi kertaakaan viikon aikana, sähkön hinnan ollessa jatkuvasti arvon Y yli. Automaatioita suunniteltaessa kannattaakin olla todella tarkka. Voi hyvinkin olla, että jatkuvat suuret muutokset lämmityksessä tulevat lopulta kalliimmiksi, kuin jatkuvan tasalämmön ylläpito. Optimoinnin tukena on hyvä käyttää mahdollisimman paljon mittausdataa lämpötiloista ja sähkönkulutuksesta, jotta toivottuihin säästöihin olisi mahdollista päästä.

Tutkielmaa kirjoitettaessa älykotiin liittyvä uutisointi on lisääntynyt ja sähkön säästämiseenkin liittyviä uutisia älylaitteiden avulla on alettu kirjoittaa. Yle uutisoi sähkön säästämistä älylaitteiden avulla. Siinä toteutettiin helppo automaatio, jonka avulla äly-

pistorasia saadaan kytkeytymään päälle ja pois pörssisähkön hinnan mukaisesti. Toimitajakin on erittäin kriittinen toteuttamansa automaation toimintavarmuudesta. Uutisessa kuitenkin osoitetaan, että käytännössä pienen automaation toteutukseen ei vaadita kuin yksi älylaite ja muutamia sovelluksia älypuhelimeen. [67]

5.6 Muut huomiot

Toimintavarman älykodin toteuttaminen todettiin tutkielmassa mahdolliseksi. Huomattiin kuitenkin, että sen toimintavarmana pitäminen vaatii jatkuvaa ylläpitoa. Home Assistantiin julkaistaan jatkuvasti päivityksiä ja on suositeltavaa, että päivitykset olisivat ajan tasalla uusien ominaisuuksien ja lisääntyvän laitetuen vuoksi. Lisäksi ohjelmiston päivittäminen usean versionumeron yli saattaa hyvinkin rikkoo koko järjestelmän, sillä suositeltu tapa päivityksille on jatkuva päivitysten asentaminen. Monen ohjelmiston versionumeron yli päivittäminen saattaa muuttaa merkittävästi tiettyjä toiminnallisuuksia ja täten aikaisemmin toimineet automaatiot saattavat rikkoutua päivityksen yhteydessä. Tästä johtuen ennen päivittämistä on suositeltavaa lukea tarkasti muutosloki, jossa mainitaan mahdollisesti tiettyjä toiminnallisuuksia rikkovista ominaisuuksista ja muista järjestelmän toiminnallisuuteen vaikuttavista seikoista.

Luku 6

Yhteenveto

Tutkielmassa suunniteltiin ja toteutettiin toimintavarma ja vakaa älykotijärjestelmä, joka perustuu ilmaiseen Home Assistant -järjestelmään. Erilaisten laitteiden lisääminen järjestelmään saatiin mahdolliseksi esimerkiksi asentamalla uusi ohjelmisto IoT-laitteisiin, mikä kasvatti myös kyberturvallisuutta. Järjestelmän käyttömukavuus saatiin säilytettyä siten, että järjestelmän käyttö on silti kyberturvallista.

Havaittiin, että järjestelmän käyttäminen vaatii jatkuvaa ylläpitoa ja päivityksien asentamista, jotta se pysyy toimintakunnossa. Lisäksi järjestelmästä on hyödyllistä ottaa jatkuvasti varmuuskopioita, jotta ongelmatilanteen sattuessa edellisen toimivan tilan palauttaminen varmuuskopiosta on mahdollista. Tutkielmassa toteutetun järjestelmän varmuuskopiot siirtyvät automaattisesti öisin internetin pilvipalveluun salasanalla suojattuina. Ennen isompia päivityksiä järjestelmän virtuaalikoneesta otetaan manuaalinen varmuuskopio paikalliselle NAS-palvelimelle. Tämän varmuuskopion palauttaminen ongelmatilanteessa on erittäin helppoa, sillä käytännössä se tapahtuu vain muutaman klikkauksen kautta Proxmoxin käyttöliittymästä.

Aluksi järjestelmää ajettiin Raspberry Pi -tietokoneessa, mutta huomattiin kuitenkin laitteiston asettamat rajoitteet tehojen ja vakauden suhteen. Tämän jälkeen hankittiin palvelinkoneeksi pienikokoinen ja vähän sähköä kuluttava Lenovon mini-PC. Tähän asennettiin virtuaalikonealustaksi Proxmox käyttöjärjestelmä, jonka päälle lopulta asen-

nettiin Home Assistant omaksi virtuaalikoneekseen. Tämä mahdollisti erittäin korkean käytettävyyden ja toimintavarmuuden. Lisäksi varmuuskopioiden ottamisen todettiin olevan toimivaa ja varmaa. Varmuuskopioinnilla on varauduttu myös palvelimen kovalevyn yllättävään rikkoutumiseen ja ripeään järjestelmän uudelleen käyttöönottoon. Järjestelmästä saatiin toivotunlaisesti kyberturvallinen hyödyntämällä mm. sertifikaatteja ja kaksivaiheista tunnistautumista.

Oman älykotijärjestelmän toteuttamiselle löytyy nykyään jo useita vaihtoehtoja. Eroja järjestelmissä on niin ulkonäössä kuin tuettujen laitteiden luetteloissakin. Mikäli kotiin halutaan toteuttaa hieman monipuolisempi älykotijärjestelmä, ovat Home Assistant ja openHAB hyviä vaihtoehtoja. Helpompi käytettävyys on saavutettavissa esimerkiksi Apple Homekittiä, Google Homea tai Amazon Alexaa tukevien laitteiden avulla. Näiden käyttöönotto on tehty helpoksi alustojen valmiilla sovelluksilla. Monelle älykotikäyttäjälle laitteiden integrointi näille alustoille olisi parannus useiden eri sovellusten käyttämisen sijaan.

Tutkielmassa havaittiin, että langattomatkin laitteet voivat olla erittäin toimintavarmoja. Esimerkiksi Zigbeellä kommunikoivat lämpötilasensorit ja ovianturit olivat varmatomisia. Mittaustuloksissa ei havaittu aukkoja tai poikkeavuuksia. Asunnon ominaisuuksia on mahdollista seurata ja ohjata eri osa-alueilta. Ovianturin tuottama data oli niin luotettavaa, että sen avulla oli mahdollista toteuttaa varmatoiminen eteisen valaistuksen ohjaus. Philips Hue -älyvalot ylittivät odotukset toimintavarmuudellaan. Niissä ei havaittu kertaakaan verkosta tipahtamista ja valojen ohjaus oli aina mahdollista. Ainut sensori, jonka toiminnassa olisi parantamisen varaa, oli Sonoffin liiketunnistin. Tämä laite hävisi usein verkosta ja sen uudelleen parittaminen oli erittäin vaivalloista. Havaittiin myös, että älyvalaistuksen käyttöön on mahdollista tottua hyvinkin nopeasti.

Älykotijärjestelmässä käytetyn laitteiston hankkimisesta kertyy kustannuksia. Älyvalot ovat hinnaltaan kalliimpia, kuin vastaavat tavalliset. Philips Huen GU10-kantainen monivärinen älyvalo maksaa noin 50 euroa ja yleisempi E27-kantainen valo noin 45 eu-

roa. Liiketunnistimien hinnat olivat 10-40 euroa. Pistorasioissa hintaan vaikutti se, olivatko ne kulutusta mittaavia; hinnat olivat 10-40 euroa. Ovimagneetit maksoivat alle 20 euroa kappaleelta. Järjestelmän kalleimpia hankintoja olivat: iRobot Roomba -robotti-imuri 300 euroa, Unifi AmplifiHD-reititin 150 euroa ja Lenovon tietokone 200 euroa. Omalla työllä on myös oma arvonsa.

Markkinoilla oleviin valmiisiin älykotiratkaisuihin verrattuna saavutettiin paljon laajempi erilaisten laitteiden yhteentoimivuus. Valmiit ratkaisut ovat toistaiseksi rajoittuneita tuettujen laitteiden vähäisen määrän vuoksi. Lisäksi ne tukevat heikosti toisten valmistajien laitteita. Zigbee-protokolla on hyvä esimerkki siitä, että vaikka standardi on kaikissa laitteissa sama, silti laitteet eivät välttämättä toimi yhdessä toisen valmistajan laitteiden kanssa. Valmiiden järjestelmien selvänä etuna kuitenkin on laitteiden toiminnan varmuus, esimerkiksi jos laitteessa on Homekit-tuki, se varmasti toimii muiden Homekit-laitteiden kanssa.

Diplomityössä toteutettu älykotijärjestelmä saatiin toimivaksi ja saavutettiin haluttuna lopputuloksena erimerkkisten laitteiden kyberturvallisempi käyttö yhdestä järjestelmästä.

Viitteet

- [1] Tilastokeskus. Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö. Liitetaulukko 5. Kotitaloudessa internetyhteys 2020, prosenttiosuus talouksista. verkkojulkaisu, marraskuu 14. 2021. URL https://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tau_005_fi.html, viitattu 15.11.2021.
- [2] Turku Energia. Usein kysyttyjä kysymyksiä etäluettavista sähkömittareista. verkkojulkaisu. URL <https://www.turkuenergia.fi/sahkoverkot/sahkoliittyma-ja-sahkon-mittaus/sahkon-mittaus/etaluettavat-sahkomittarit>, viitattu 20.11.2021.
- [3] Thorin Klosowski. We Asked Appliance Manufacturers How Long They'll Keep Connected Devices Secure. Many Couldn't Tell Us. verkkojulkaisu, elokuu 24. 2020. URL <https://www.nytimes.com/wirecutter/blog/how-long-connected-devices-secure/>, viitattu 20.11.2021.
- [4] Khusvinder Gill, Shuang-Hua Yang, Fang Yao ja Xin Lu. A zigbee-based home automation system. *IEEE Transactions on consumer Electronics*, 55(2):422–430, 2009.
- [5] Philips Hue. Philips Hue, viihtyisyyttä lisäävä kodin älyvalaistus. verkkojulkaisu. URL <https://www.philips-hue.com/fi-fi>, viitattu 1.2.2022.

- [6] Samsung. Samsung - SmartThings. verkkojulkaisu. URL <https://www.samsung.com/fi/smartthings/>, viitattu 24.11.2021.
- [7] Faiyaz Doctor, Hani Hagraj ja Victor Callaghan. A fuzzy embedded agent-based approach for realizing ambient intelligence in intelligent inhabited environments. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 35(1):55–65, 2004.
- [8] Michael C. Mozer. The neural network house: An environment that adapts to its inhabitants. Teoksessa *Proc. AAAI Spring Symp. Intelligent Environments*, osa 58. 1998. Boulder, Colorado, Yhdysvallat.
- [9] Lin Liao, Dieter Fox ja Henry A Kautz. Location-Based Activity Recognition using Relational Markov Networks. Teoksessa *IJCAI*, osa 5, ss. 773–778. 2005. Seattle, Washington, Yhdysvallat.
- [10] Richard Harper. *Inside the smart home*. Springer Science and Business Media, 2006. Lontoo, Yhdistynyt kuningaskunta.
- [11] Hedengren. HHL-rikosilmoitinjärjestelmä. verkkojulkaisu. URL <https://www.hedengren.com/fi/turvatekniikka/murtohalyttimet>, viitattu 23.08.2022.
- [12] Terhi Vuorinen ja Maarit Åström. Vertailimme kodin murtohälytysjärjestelmiä: hinnoissa ja palveluissa tuntuja eroja. verkkojulkaisu. URL <https://yle.fi/aihe/artikkeli/2017/01/25/vertailimme-kodin-murtohalytysjarjestelmia-hinnoissa-ja-palveluissa-tuntuja>, viitattu 20.2.2022.
- [13] Riikka Nykänen. Aftonbladet: Skandaali Verisussa: työntekijöiden kerrotaan katselleen asiakkaiden alastonkuvia – yhtiö selvittää. verkkojulkaisu. URL <https://www.is.fi/digitoday/art-2000008769860.html>, viitattu 23.4.2022.

- [14] David Gann, James Barlow ja Tim Venables. *Digital Futures: making homes smarter*. Chartered Institute Of Housing, 1999. Coventry, Yhdistynyt kuningaskunta.
- [15] Lou Harry ja Sam Stall. *As Seen on TV: 50 Amazing Products and the commercials that made them famous*. Quirk Books, 2002. Philadelphia, Pennsylvania, Yhdysvallat.
- [16] Sector Alarm. Älykodin laitteet. verkkojulkaisu. URL <https://www.sectoralarm.fi/alykodin-laitteet/>, viitattu 21.08.2022.
- [17] Verisure. Älykoti. verkkojulkaisu. URL <https://www.verisure.fi/alykoti>, viitattu 21.08.2022.
- [18] Apple. Your home at your command. verkkojulkaisu. URL <https://www.apple.com/ios/home/>, viitattu 22.3.2022.
- [19] Amazon. Alexa features. verkkojulkaisu. URL <https://www.amazon.com/alexa>, viitattu 22.3.2022.
- [20] Google. Meet your Google Assistant. verkkojulkaisu. URL https://assistant.google.com/intl/en/_ca/, viitattu 22.3.2022.
- [21] Home Assistant. Home Assistant. verkkojulkaisu. URL <https://www.home-assistant.io/>, viitattu 21.11.2021.
- [22] Domoticz. Domoticz - Control at your fingertips. verkkojulkaisu. URL <https://www.domoticz.com/>, viitattu 22.3.2022.
- [23] openHAB. openHAB - empowering the smart home. verkkojulkaisu. URL <https://www.openhab.org>, viitattu 22.3.2022.
- [24] Raspberry Pi Foundation. Raspberry Pi 3 Model B+. verkkojulkaisu. URL <https://www.raspberrypi.com/products/raspberry-pi-3-model-b-plus/>, viitattu 1.5.2022.

- [25] Eric Brown. Home Assistant: The Python Approach to Home Automation. verkkojulkaisu. URL <https://www.linux.com/topic/embedded-iot/home-assistant-python-approach-home-automation>, viitattu 24.3.2022.
- [26] Ville Harkke, Dario Alessi ja Mikael Collan. IT and institutional constraints: effects of legal and administrative constraints to use it in production of health care services-focus on Finland. Teoksessa *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, ss. 6–pp. IEEE, 2003. Big Island, Havaiji, Yhdysvallat.
- [27] Davar Pishva ja Keiji Takeda. Product-based security model for smart home appliances. *IEEE Aerospace and Electronic Systems Magazine*, 23(10):32–41, 2008.
- [28] Wang Wei. Linux Trojan Using Hacked IoT Devices to Send Spam Emails. verkkojulkaisu. URL <https://thehackernews.com/2017/09/linux-malware-iot-hacking.html>, viitattu 13.11.2022.
- [29] Somayya Madakam, R. Ramaswamy ja Siddharth Tripathi. Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, 3(05), 2015. Mumbai, Intia.
- [30] Jan Bauwens, Peter Ruckebusch, Spilios Giannoulis, Ingrid Moerman ja Eli De Poorter. Over-the-air software updates in the internet of things: An overview of key principles. *IEEE Communications Magazine*, 58(2):35–41, 2020.
- [31] Ubiquiti Inc. Amplifi. verkkojulkaisu. URL <https://amplifi.com/amplifi-hd>, viitattu 20.4.2022.
- [32] pfSense. pfSense - World's Most Trusted Open Source Firewall. verkkojulkaisu. URL <https://www.pfsense.org>, viitattu 20.4.2022.

- [33] Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini ja Rodrigo de Oliveira. Your browsing behavior for a big mac: Economics of personal information online. Teoksessa *Proceedings of the 22nd international conference on World Wide Web*, ss. 189–200. 2013. New York, New York, Yhdysvallat.
- [34] Shashi Kiran, Patricia Lareau ja Steve Lloyd. PKI Basics-A Technical Perspective. Teoksessa *PKI-Forum*. 2002.
- [35] Jae-Jung Kim ja Seng-Phil Hong. A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, 7(1):187–198, 2011.
- [36] Bruce Schneier. Two-factor authentication: too little, too late. *Communications of the ACM*, 48(4):136, 2005.
- [37] Weizhi Meng, Duncan S Wong, Steven Furnell ja Jianying Zhou. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys Tutorials*, 17(3):1268–1293, 2015.
- [38] Gerard Draper-Gil, Arash Habibi Lashkari, Mohammad Saiful Islam Mamun ja Ali A Ghorbani. Characterization of encrypted and vpn traffic using time-related. Teoksessa *Proceedings of the 2nd international conference on information systems security and privacy (ICISSP)*, ss. 407–414. sn, 2016. Fredericton, New Brunswick, Kanada.
- [39] Klaus Schmeh. *Cryptography and public key infrastructure on the Internet*. John Wiley & Sons, 2006.
- [40] Bruce Perens. The open source definition. *Open sources: voices from the open source revolution*, 1:171–188, 1999.
- [41] OpenVPN. Installing OpenVPN Access Server on a Linux system. verkkojulkaisu. URL <https://openvpn.net/vpn-server->

resources/installing-openvpn-access-server-on-a-linux-system/, viitattu 20.1.2022.

- [42] David Naylor, Alessandro Finamore, Ilias Leontiadis, Yan Grunenberger, Marco Mellia, Maurizio Munafò, Konstantina Papagiannaki ja Peter Steenkiste. The cost of the "S" in https. Teoksessa *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, ss. 133–140. 2014. New York, New York, Yhdysvallat.
- [43] Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. Alex Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla et al. Let's Encrypt: an automated certificate authority to encrypt the entire web. Teoksessa *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ss. 2473–2487. 2019. New York, New York, Yhdysvallat.
- [44] Letsencrypt. About Let's Encrypt. verkkojulkaisu. URL <https://letsencrypt.org/about/>, viitattu 22.1.2022.
- [45] Letsencrypt. How it works. verkkojulkaisu. URL <https://letsencrypt.org/how-it-works/>, viitattu 22.5.2022.
- [46] Duck DNS. Duck DNS - free dynamic DNS hosted on AWS. verkkojulkaisu. URL <http://www.duckdns.org>, viitattu 1.5.2022.
- [47] Home Assistant. Home Assistant Add-on: DuckDNS. verkkojulkaisu. URL <https://github.com/home-assistant/addons/blob/master/duckdns/DOCS.md>, viitattu 1.5.2022.
- [48] Home Assistant. Home Assistant - Dashboards. verkkojulkaisu. URL <https://www.home-assistant.io/dashboards/>, viitattu 02.04.2022.

- [49] Lenovo. ThinkCentre M600 Tiny PC - Powerful Micro Desktop - Lenovo. verkkojulkaisu. URL <https://www.lenovo.com/au/en/desktops-and-all-in-ones/thinkcentre/m-series-tiny/M600-Tiny/p/11TC1MTM600>, viitattu 1.5.2022.
- [50] VMware. What is ESXi. verkkojulkaisu. URL <https://www.vmware.com/products/esxi-and-esx.html>, viitattu 4.2.2022.
- [51] Roberto Morabito, Jimmy Kjällman ja Miika Komu. Hypervisors vs. lightweight virtualization: a performance comparison. Teoksessa *2015 IEEE International Conference on Cloud Engineering*, ss. 386–393. IEEE, 2015. Tempe, Arizona, Yhdysvallat.
- [52] VMware. VMware Compatibility Guide. verkkojulkaisu. URL <https://www.vmware.com/resources/compatibility/search.php>, viitattu 4.2.2022.
- [53] Proxmox. Proxmox - Powerful open-source server solutions. verkkojulkaisu. URL <https://proxmox.com/en/>, viitattu 1.5.2022.
- [54] Stanislav Safaric ja Kresimir Malaric. ZigBee wireless standard. Teoksessa *Proceedings ELMAR 2006*, ss. 259–262. IEEE, 2006. Zadar, Kroatia.
- [55] Tinku Kumar ja PB Mane. ZigBee topology: A survey. Teoksessa *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, ss. 164–166. IEEE, 2016. Kumarakoil, Intia.
- [56] Robin Heydon. Bluetooth Low Energy: The Developer's Handbook. s. 3, 2013.
- [57] Mat Zolnierczyk. Flashing CC2531 without CC Debugger. verkkojulkaisu. URL <https://notenoughtech.com/home-automation/flashing-cc2531-without-cc-debugger/>, viitattu 10.3.2022.

-
- [58] ThingSpeak. ThingSpeak for IoT Projects. verkkojulkaisu. URL <https://thingspeak.com>, viitattu 3.3.2022.
- [59] MQTT. MQTT: The Standard for IoT Messaging. verkkojulkaisu. URL <https://mqtt.org/>, viitattu 3.3.2022.
- [60] Aircoookie. WLED Project. verkkojulkaisu. URL <https://kno.wled.ge/>, viitattu 1.2.2022.
- [61] Tasmota. Open source firmware for ESP devices. verkkojulkaisu. URL <https://tasmota.github.io/docs/>, viitattu 2.2.2022.
- [62] ESPHome. Install Tasmota. verkkojulkaisu. URL <https://tasmota.github.io/install/>, viitattu 2.3.2022.
- [63] blakadder. IKEA Vindriktning air quality sensor running Tasmota. verkkojulkaisu. URL <https://blakadder.com/vindriktning-tasmota/>, viitattu 2.5.2022.
- [64] Osram. The lightify cloud servers will be switched off on August 31th 2021. verkkojulkaisu. URL <https://www.osram.com/cb/lightify/index.jsp>, viitattu 1.2.2022.
- [65] David Nield. The original, 1st-gen Philips Hue Bridge goes dark on April 30. verkkojulkaisu. URL <https://www.techradar.com/news/the-original-1st-gen-philips-hue-bridge-goes-dark-on-april-30>, viitattu 2.2.2022.
- [66] Raluca Budiu. Nielsen Norman Group. *Mobile: Native Apps, Web Apps, and Hybrid Apps*, ss. 49–53, 2013.

-
- [67] Juha-Matti Mäntylä. Analyysi: Näin helposti 20 euron pistorasian saa syttymään ja sammumaan pörssisähkön tahdissa. verkkojulkaisu. URL <https://yle.fi/uutiset/3-12633301>, viitattu 10.10.2022.