VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Sonja Myllymäki

IoT-automaatiojärjestelmän tietoturvan parantaminen

Tekniikka
2024

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Sonja Myllymäki
Opinnäytetyön nimi	IoT-automaatiojärjestelmän tietoturvan parantaminen
Vuosi	2024
Kieli	suomi
Sivumäärä	50
Ohjaaja	Aleksi Ukkola

Tämän opinnäytetyön tarkoituksena oli tutustua IoT:in eli esineiden internetiin sekä sen soveltamiseen kotiautomaatiojärjestelmässä. Tutkimuksen painopiste on IoT-verkkojen tietoturvassa, uhkatekijöissä ja kuinka sitä pyritään parantamaan erinäisin keinoin. Kotiautomaatiojärjestelmää varten tutustuttiin Home Assistant -kotiautomaatio-ohjelmistoon sekä älykomponentteihin kuten valaisimiin.

Opinnäytetyössä selvitettiin IoT:n arkkitehtuuria, sen kerroksia ja niiden tehtäviä. Lisäksi tutustuttiin IoT-järjestelmien suurimpiin uhkiin ja haavoittuvuuksiin sekä kuinka esimerkiksi eri standardit, kuten Zigbee, pyrkivät niiltä verkkoa suojaamaan. Standardeista erityistarkastelussa oli Matter, joka on uusin tulokas sillä saralla.

Kotiautomaatiojärjestelmän toteutuksessa hyödynnettiin eri valmistajien Matter-tuen omaavia komponentteja ja luotiin näin yhtenäinen järjestelmä, joka osaltaan vastaa IoT-verkon turvallisuushuoliin. Tutkimusaineistossa kun todettiin usean standardin heikentävän tietoturvaa. Yhä useamman kuluttajan rakentaessa omaa IoT-järjestelmää kotinsa verkkoon, on asiantuntemuksen puutteesta johtuvien, tahattomien tietoturva-aukkojen syntyminen todennäköistä. Tähän uhkaan Matter tuo helpotusta vähentämällä järjestelmien monimutkaisuutta.

Avainsanat	esineiden internet, tietoturva, langattomat verkot, älytekniikka

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Sonja Myllymäki
Title	Enhancing the Security of IoT Automation Systems
Year	2024
Language	Finnish
Pages	50
Name of Supervisor	Aleksi Ukkola

The purpose of this thesis was to explore the Internet of Things (IoT) and its application in home automation systems. The focus of the research is on the security of IoT networks, threats, and how they are addressed through various means. For the home automation system, the study examined the Home Assistant home automation software and smart components such as lighting fixtures.

The thesis investigated the architecture of IoT, its layers, and their functions. Additionally, it explored the major threats and vulnerabilities of IoT systems, as well as how various standards, such as Zigbee, aim to protect the network from them. Matter, the newest entrant in this field, was specifically examined among the standards.

In the implementation of the home automation system, components from various manufacturers with Matter support were utilized to create a unified system, which contributes to addressing concerns regarding the security of IoT networks. The research findings indicated that several standards weaken security. As more consumers build their own IoT systems on their home networks, the likelihood of unintentional security vulnerabilities due to lack of expertise increases. Matter addresses this threat by simplifying system complexity.

Keywords Internet of things, data security, wireless networks, intelligent systems

SISÄLLYS

KUVA- JA TAULUKKOLUETTELO

1 JOHDANTO

Teknologia kehittyy jatkuvasti ja monet arkeemme saumattomasti kuuluvat asiat ovat joskus olleet kaukaista tulevaisuutta, jopa utopiaa, joista etenkään alaan vihkiytymätön ei ole edes osannut haaveilla. Viime vuosituhannen elokuva-ala kuitenkin maalasi kuvaa tulevaisuudesta myös realistiseksi osoittautuneella tavalla: esimerkiksi vuonna 1982 ilmestynyt Blade runner -elokuva esitteli muun muassa digitaaliset mainostaulut sekä videopuhelut. (Vedenpää, 2019) Näiden lisäksi elämäämme on tullut monia muita tuolloin fantasiaksi luettuja ulottuvuuksia: voimme tarkistaa jääkaappimme sisällön kaupassa ollessamme, käynnistää kahvinkeittimen sängystä käsin, säätää sekä automatisoida valaistusta tai lämpötilaa esimerkiksi tilojen käytön mukaan, sekä käyttää monia muita arkeamme helpottamaan kehitettyjä ominaisuuksia. Tämän meille mahdollistaa esineiden internetiksi kutsuttu IoT (Internet of Things). Sen yleistymisestä kertoo Euroopan komission nettisivuillaan julkaisema arvio, jonka mukaan vuonna 2023 esineitä oli liitetty internetiin 40 miljardia, ja vuoteen 2026 mennessä määrän odotetaan olevan jo 49 miljardia. (European Comission, n.d.)

Esineiden internetistä puhuttaessa ei voida unohtaa tietoturvan merkitystä. Verkon laitteet on suojattava niin ettei ulkopuolisilla ole mahdollisuutta päästä käsiksi niihin, saati niiden keräämään dataan. Siksi opinnäytetyön aiheena on tutkia IoT-verkon tietoturvan tilaa nyt ja kuinka sitä pyritään parantamaan. Työssä perehdytään IoT:n rakenteeseen, miksi ja miten tietoturva tulee huomioida, ja millaisin työkaluin. Tutustutaan vuonna 2022 julkaistuun Matter-teknologiaan ja tutkitaan, mitä hyötyjä se tuo IoT-automaatiokentälle. Tutkimuksen lisäksi rakennetaan älykotijärjestelmä pienyrityksen toimistoon. Järjestelmää varten luodaan oma palvelin sisäverkkoon. Alustana käytetään Home Assistant -kotiautomaatio-ohjelmistoa.

2 IOT - INTERNET OF THINGS

Internet of things eli esineiden internet, tarkoittaa nimensä mukaisesti esineiden, liittämistä internetiin. Esine voi olla mikä tahansa verkkoyhteyttä hyödyntävä kodinesine, esimerkiksi kodinkone, puettavaa teknologiaa kuten älykello tai jopa auto. Esineiden lisäksi verkkoon voidaan yhdistää myös kokonaisia kiinteistöjä ja kaupunkeja. (Pörhölä, 2017) IoT:n tarkoitus on yhdistää siihen kytkettyjä laitteita, antureita sekä järjestelmiä, jotta ne pystyvät kommunikoimaan ja jakamaan dataa sovelluksien kuten etäseurannan, laitteiden etähallinnan ja älykkäiden ratkaisujen kehittämiseksi. Jari Uppa (2017) kuvaa IoT:n toimintaa seuraavasti:

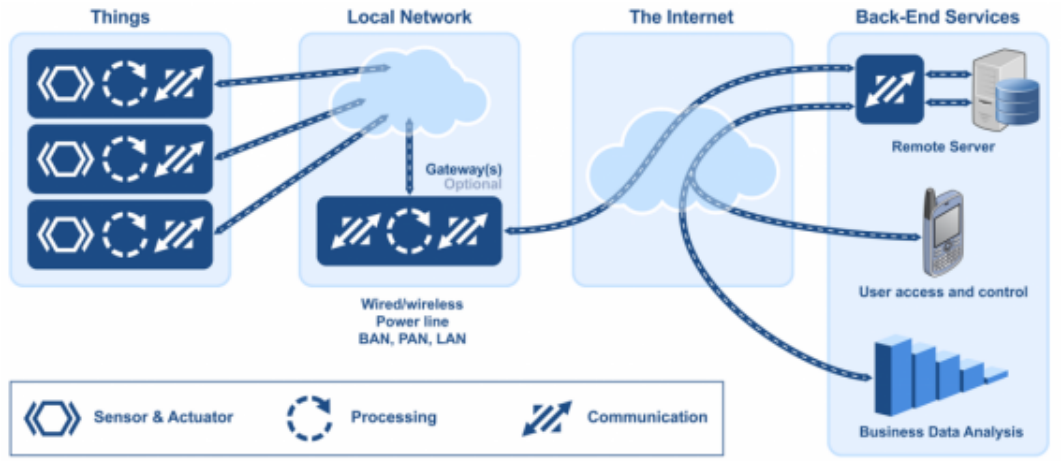
> Ne (esineet) lähettävät joko omasta tilastaan tai ympäristöstään erilaisilla sensoreilla keräämäänsä tietoa tyypillisesti pilvipalveluun, jossa laitteiden välittämää raakadataa voidaan analysoida ja visualisoida. Laitteet voivat kommunikoida verkon välityksellä sekä toisten laitteiden, että ihmisten kanssa. Esineiden internetin liikenne on tyypillisesti kaksisuuntaista ja se mahdollistaa lisäksi laitteiden etäohjauksen ja niiden ohjelmistojen päivittämisen. (Uppa, 2017, s. 8)

IoT:ä hyödyntävä järjestelmä sisältää siis usein myös antureita sisältäviä mittauslaitteita, joiden avulla voidaan seurata esimerkiksi ihmisen elämäntapoja (aiemmin mainittu älykello) tai rakennusten energiankulutusta. IoT-sovellusten avulla on mahdollista ohjata ja säätää laitteita niistä saadun valvontadatan perusteella. (Logistiikan maailma, n.d.)

Kuluttajien lisäksi myös teollisuus hyötyy esineiden internetistä. IoT kehitettiin alun perin teollisuusympäristöjä varten, mutta sen laajennuttua kuluttajatuotteisiin, teollisuudessa otettiin käyttöön uusi termi, IIoT eli Industrial Internet of Things. (Väisänen, 2019) Teollinen internet on mullistanut teollisuuden alan ja sitä kutsutaankin teollisen vallankumouksen neljänneksi aalloksi. (Oracle, n.d.) Tässä opinnäytetyössä keskitytään kuitenkin IoT:in.

IoT:n nopeaa kasvua on edesauttanut vuonna 2011 lanseerattu IPv6-protokolla. Nykyisessä digitaalisessa maailmassa aiemman IPv4-protokollan tarjoamat noin

neljä biljoonaa julkista IP-osoitetta alkoivat käydä vähiin, joten IPv6:n käyttöönotto kasvatti osoiteavaruutta lisäämällä siihen noin 340 sekstiljoonaa osoitetta ja mahdollistaen näin yhä useamman laitteen kytkemisen verkkoon. (Myllyaho, 2020) Kuvassa 1 on esitetty tyypillinen IoT-verkko.



Kuva 1. Tyypillisen IoT-verkon rakenne. (Uppa, 2017, s. 16)

2.1 Arkkitehtuuri

Esineiden internetissä avainasemassa on sen arkkitehtuuri, joka yhdistää laitteet, anturit sekä sovellukset yhdeksi toimivaksi järjestelmäksi. Sillä on suuri merkitys IoT-teknologioiden hankkiman tiedon tehokkaassa hallinnassa ja hyödyntämisessä esimerkiksi vianetsintään järjestelmästä. Arkkitehtuuria kuvataan kerrosten avulla. Vähimmäisvaatimus on neljä kerrosta: laitekerros, yhteyskerros, tiedon käsittelykerros ja sovelluskerros. (José, 2023) Tarkimmassa mallissa kerroksia on seitsemän, kuten kuvassa 2 on esitetty. Arkkitehtuuri rakentuu järjestelmän toimivuusvaatimusten ja tarkoituksen mukaan.

Lähteestä riippuen arkkitehtuurin rakennus neljän pääkerroksen ympärille on kuvattu hieman eri järjestyksessä ja eri sanoin. Seuraavassa tiivistelmä jokaisesta seitsemästä kerroksesta.

Kuva 2. IoT-arkkitehtuuri rakentuu järjestelmän toimivuusvaatimusten ja tarkoituksen mukaan vähintään neljästä ja enintään seitsemästä kerroksesta.

2.1.1 Laitekerros

Laitekerros koostuu nimensä mukaisesti fyysisistä laitteista, antureista ja ympäristöä havainnoivista sulautetuista järjestelmistä. Kerros on yksi tärkeimmistä, sillä sen tehtävä on kerätä data, jota ylemmissä kerroksissa käsitellään. Käyttötarkoituksen mukaan, data voi olla esimerkiksi mittaustuloksia tilan lämpötilasta, kosteudesta, valosta ja äänestä tai tietoa jonkin laitteen toiminnasta. Adam Simmons (2022) antaa esimerkin artikkelissaan Internet of Things (IoT) Architecture: Layers Explained: autojen kokoonpanolinjalle asennettua anturia voidaan käyttää valvomaan sulakerasioita kokoavaa robottia. Anturi tarkistaa jokaisen kootun sulakkeen

asennon niiden värikoodauksen avulla ja suorittaa näin laadunvalvontaa. Saatu data välitetään muihin kerroksiin, jossa se käsitellään.

Laitteet kytketään verkkoon yhteyskerroksen langallisen tai langattoman tiedonsiirtoprotokollan kautta. (Geeks for geeks, n.d.)

2.1.2 Yhteyskerros

Yhteyskerrosta kutsutaan myös verkkokerrokseksi. Se sisältää tiedonsiirtoprotokollia kuten MQTT, Modbus ja verkkoteknologioita kuten Wi-Fi, Bluetooth, Zigbee sekä verkkolaitteita kuten reitittimiä. Yhdessä ne huolehtivat sekä verkon laitteiden välisestä että verkon ulkopuolisesta liikenteestä.

Kerroksen vastaanottaessa dataa IoT-laitteelta, data muunnetaan analogisesta digitaaliseen muotoon. Muuntamisen jälkeen data lähetetään tarpeeseen sopivan tiedonsiirtoprotokollan avulla tietokeskukseen. Tiedonsiirtoprotokollan valintaan vaikuttaa esimerkiksi lähetettävän datan koko ja tyyppi sekä verkkoyhteyden luotettavuus. (Simmons, 2022)

Ulkoiseen verkkoon liityttäessä on huomioitava sen aiheuttamat riskit tietoturvan kannalta, joten verkkokerrokseen sisällytetään usein myös turvallisuudesta huolen pitäviä ominaisuuksia ja tarkastuksia kuten käyttäjän tunnistaminen. (Geeks for geeks, n.d.) Yhteyskerros sisältää lisäksi tiedonhankintajärjestelmän, joka mahdollistaa antureilta kerätyn tiedon jakamisen järjestelmän sovellusten välillä. (José, 2023)

2.1.3 Reunalaskentakerros

Mitä enemmän verkossa on liikennettä sitä suurempi riski on viiveille. Verkon laitteiden lisääntyessä liikenteen määrä luonnollisesti kasvaa. Vaikka suurin osa liikenteestä kulkee pilvipalveluiden kautta, on suorituskyvyn ongelmien ja viiveiden välttämiseksi kehitetty reunalaskentatekniikka, joka pyrkii käsittelemään ja analy-

soimaan dataa mahdollisimman lähellä sen alkuperäistä lähdettä, jolloin IoT-verkkoon siirrettävän datan määrä pienenee. (Myllyaho, 2020) Tämä tehdään reunalaskenta- (eng. edge computing) sekä reunayhdyskäytävälaitteiden (eng. edge gateway) avulla. Reunalaskentalaite kerää dataa tietystä ympäristöstä tai järjestelmästä. Simmonsin (2023) mukaan laite voi olla, mikä tahansa IoT-anturi, jos sen tallennus- ja laskentateho riittää suodattamaan tai käsittelemään tietoja paikallisesti muutamassa millisekunnissa. (Simmons, 2023) Se voi olla esimerkiksi kamera, joka pystyy laskemaan kuvaamassaan videossa esiintyvien ihmisten lukumäärän käyttäen videoanalysointiominaisuuksiaan.

Reunayhdyskäytävälaite sijaitsee reunalaskentalaitteen ja muun IoT-verkon välissä, jossa se käsittelee ja suodattaa reunalaskentalaitteen datan ja välittää sen määritettyyn paikkaan, kuten pilvialustalle. Jotkin reunalaskentalaitteet voivat suorittaa myös itse datan käsittelyn sekä suodatuksen. (Simmons, 2023) Arkkitehtuurin näkökulmasta laitteet sijaitsevat ensimmäisessä eli laitekerroksessa.

2.1.4 Tiedon käsittelykerros

Kerätty data käsitellään tiedon käsittelykerroksessa ohjelmisto- ja laitteistokomponenttien avulla. Komponentit keräävät, analysoivat ja tulkitsevat kerättyä ”raakatietoa” hyödyntäen tiedon hallintajärjestelmiä, analytiikka-alustoja sekä koneoppimisalgoritmeja. (Geeks for geeks, n.d.) Toisin sanoen ”raakatieto” pureskellaan osittain valmiiksi seuraavien kerrosten työn helpottamiseksi. Louise Josén (2023) mukaan yritykset voivat saada esikäsittelystä konkreettista apua: dataa käsitellään ja analysoidaan auttamaan yrityksiä päätöksenteossa sekä toimintojen tehostamisessa. Kerros voi käsitellä IoT-järjestelmistä saatua raakatietoa koneoppimisalgoritmien avulla säilyttääkseen automatisoidun päätöksenteon kannalta hyödylliset yksityiskohdat. (José, 2023)

Kun IoT-verkossa on useita laitteita, käsittelee se suuria määriä erilaista dataa. Termi ”väliohjelmisto” (eng. middleware) tarkoittaa ohjelmistoa, joka mahdollis-

taa viestinnän erilaisten ohjelmistojen ja tietojärjestelmien välillä. (IBM, n.d.) Väliohjelmiston avulla IoT-järjestelmän on mahdollista hallita sen käsittelykerrokselle saapuvaa monen tyyppistä dataa. Adam Simmons (2022) listaa kolme vaihetta, joita väliohjelmisto käyttää valmistellessaan dataa sovelluskerrokselle lähetystä varten:

1. datan kertyminen: datatyypin tunnistaminen ja tallentaminen sille sopivaan varastoon. Rakenteellinen data kuten mittaukset tallennetaan tietovarastoihin (eng. data warehouse), rakenteeton puolestaan datajärviin
2. datan abstraktio: datan yhdistäminen useista lähteistä ja sen luettavuuden varmistaminen sovelluskerroksessa odottavalle ohjelmistolle
3. data-analyysi: suurista ja satunnaisista tietojoukoista kuvioiden havaitsemiseen erikoistuneiden koneoppimis- (ML) tai syväoppimisalgoritmien (DL) käyttäminen.

Kohdassa yksi mainittu datajärvi on datan tallennusteknologia. Tuija Tamminen (2022) kuvaa teknologiaa seuraavasti: ”datajärvi on datan tallennukseen luotu alusta ja sinne voidaan tallentaa sekä strukturoimatonta että strukturoitua dataa. Se voi olla hyvä vaihtoehto suurten ja yksinkertaisten tietojoukkojen käsittelyyn.” (Tamminen, T., 2022)

2.1.5 Sovelluskerros

Sovelluskerros on tärkeimmistä kerroksista ylin ja käyttäjälle näkyvin: kerros huolehtii käyttöliittymien ja toimintojen käyttäjäystävällisyydestä eli mahdollistaa loppukäyttäjälle IoT-laitteiden hallinnan esimerkiksi mobiilisovelluksen tai web-portaalin kautta. Kerros voi sisältää myös koneoppimisalgoritmeja, tietojen visualisointityökaluja ja muita edistyneitä analytiikkaominaisuuksia parantaakseen datan ymmärrettävyyttä loppukäyttäjälle. (Geeks for geeks, n.d.) Opinnäytetyössä myöhemmin käsiteltävä kotiautomaatiojärjestelmä on yksi esimerkki, kuinka sovelluskerros hyödyttää loppukäyttäjää.

2.1.6 Hallintokerros

Hallintokerrosta kutsutaan myös esimerkiksi nimellä liiketoimintakerros. Sen tarkoitus on yhdistää kaikki alemmilla tasoilla suoritetut prosessit käytettäväksi kokonaisuudeksi: ”laitteiden keräämästä datasta jalostettua tietoa voidaan käyttää esimerkiksi liiketoimintaprosessien apuna tai muulla tavalla, joka hyödyttää järjestelmän käyttäjiä.” (Uppa, 2017)

2.1.7 Turvallisuuskerros

Turvallisuuskerros kulkee kaikkien arkkitehtuurin kerrosten läpi, sillä se pitää huolen koko IoT-järjestelmän turvallisuudesta. Kerroksessa suojellaan IoT-laitteita, pilvipalveluja sekä kaikkia komponentteja yhdistäviä yhteyksiä. (Simmons, 2022) Tärkeitä keinoja turvallisuuden ylläpidossa ovat esimerkiksi salasanojen käyttö laitteissa, käyttöoikeuksien hallinta sekä palomuurit.

2.2 Verkkoteknologiat

Arkkitehtuurin yhteyskerroksessa mainittiin verkkoteknologiat. Laitekerroksen laitteet liitetään IoT-järjestelmään erilaisten verkkoteknologioiden avulla. Esimerkkeinä mainittiin muun muassa Bluetooth sekä Zigbee, jotka ovat lyhyen kantaman teknologioita, ja erityisesti Bluetooth on siksi tuttu esimerkiksi älykellojen käyttäjille. Verkkoteknologioille yhteistä on pyrkimys vähäiseen virrankulutukseen laitteiden ollessa usein paristo- tai akkukäyttöisiä, joten teknologioille ominainen jako onkin erotella ne kantaman perusteella. Pitkän kantaman verkkoteknologioita ovat esimerkiksi LoRaWAN, joka on ”vähävirtainen ja suunniteltu pienten datamäärien lähettämiseen ja vastaanottamiseen” (Hagelberg, 2021) sekä NB-IoT, joka sopii myös yllä mainittuun kuvaukseen, mutta toimii operaattorien matkapuhelinverkkotaajuuksilla, samalla kun LoRaWAN käyttää matalia taajuuksia. Koska opinnäytetyön aiheena on kotiautomaatiojärjestelmä, keskitytään jatkossa lyhyen kantaman verkkoteknologioihin.

Vaaditun kantaman lisäksi verkkoteknologian valintaan vaikuttaa myös laitteiden keräämän ja välittämän datan määrä sekä laitteiden valvonta- ja ohjaus tarkoituksissa yhteysteknologian soveltuminen kaksisuuntaiseen liikenteeseen. (Uppa, 2017)

3 TIETOTURVA

Tietosuojavaltuutetun toimisto määrittelee tietoturvan seuraavasti: ”tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.” (Tietosuojavaltuutetun toimisto, n.d.) Luottamuksellisuus tarkoittaa arkaluonteisten tietojen kuten henkilö- tai terveystietojen säilyttämistä niin, etteivät ne päädy ulkopuolisten nähtäville. Eheys liittyy vahvasti luottamuksellisuuteen: datan eheys säilyy, kun sitä voi muokata vain siihen oikeutettu henkilö.

Yksityistalouksissa käytettävien teknologioiden lisääntyessä, kohdataan myös uusia uhkia ja riskejä. Kun useat kodinlaitteet liitetään internetiin kotitalouden oman verkon kautta, pienikin tietoturva-aukko avaa hyökkääjälle monia mahdollisuuksia. Jo asennusvaiheessa piilee riskejä, kun ”maallikko asentaa langatonta verkkoa tehdasasetuksilla tai vanhalla laitteistolla, verkkoon saattaa jäädä tietoturva-aukkoja, joita asiaan perehtynyt henkilö voi käyttää hyväkseen.” (Sissala, 2021)

3.1 Historia ja nykytilanne

IoT-laitteiden suosion alkuhetkillä, 2010-luvun taitteessa, aiemmin Applen iPhone-laitteiden kehityksessä työskennellyt Tony Fadell kehitti Nest Lerning -termostaatin, joka oli ensimmäinen älykäs termostaatti (Fadell, 2022). Googlen ostettua termostaatin vuonna 2014, sai se aikaan aallon, jonka myötä useat yritykset kehittivät ja julkaisivat omia IoT-laitteitaan sivuuttaen kiirehtiessään laitteiden tietoturvaa koskevat huolet. Vei lähes 10 vuotta, että turvallisuus- ja yksityisyyssääntöjä säätävät virastot kuten maailmanlaajuinen matkapuhelinoperaattoreiden edustaja GSMA ja Yhdysvaltain kauppakomissio FTC alkoivat tiukentaa sääntöjä. (Myllyaho, 2020)

IoT-laitteisiin kohdistuvien hyökkäysten ajatellaan saaneen alkunsa vuoden 2016 Mirai-hyökkäyksestä, joka hyödynsi bottiverkkoa DDoS-hyökkäyksensä levittämiseen. Bottiverkoksi kutsutaan hakkerin kaappaamien laitteiden verkostoa, jonka tarkoituksena Mirai-hyökkäyksessä oli suorittaa palvelunestohyökkäyksiä (DDoS) eli estää tietyn verkkosivun tai palvelun käyttö ruuhkauttamalla ja romahduttamalla se saastuneiden laitteiden avulla. Mirai käytti IoT-laitteiden tietoturva-aukkoja levittääkseen itsestään monistuvaa matoa, jonka avulla se valjasti laitteet osaksi bottiverkkoaan. (Myllyaho, 2020) Mirai toimii edelleen pohjana hyökkäyksille: viimeisimpänä vuonna 2024 tietoturva-asiantuntijoiden ryhmä havaitsi uuden Mirai-variaation nimeltä NoaBot, joka levittää kryptolouhintahaittaohjelmaa salattuun tietoliikenteeseen tarkoitetun SSH-protokollan avulla. (Vaughan-Nichols, 2024)

Kotiautomaation yleistyessä myös hyökkäysriskissä olevien laitteiden määrä kasvaa. Tässä opinnäytetyössä myöhemmin rakennettavan kotiautomaatiojärjestelmän yhtenä komponenttina tulee toimimaan Philips Hue-älyvalo, jota on käytetty Chain Reaction -nimisessä akateemisessa tutkimuksessa, jossa kyseiseen valoon hyökättiin sen käyttämän Zigbee-protokollan avulla. (Myllyaho, 2020) Ari Paasonen (2017) kertoo hyökkäyksestä tarkemmin:

> Hyökkäys oli mahdollista toteuttaa yli 300m etäisyydeltä asentaen muokatun firmwaren laitteille ja estäen järjestelmän päivitysmahdollisuuden tulevaisuudessa. Tämä tarkoittaa myös sitä, ettei haitallista firmwarea ole mahdollista poistaa kyseisiltä laitteilta tulevaisuudessa. (Paasonen, 2017, s. 14)

Älyvalon ideana on luoda käyttäjälle mahdollisuus hallita valaisimen toimintaa esimerkiksi säätämällä lämpötilaa, ajastamalla valaistusta eri ajankohtiin tai synkronoimalla se reagoimaan musiikin tahtiin. Hyökkäys iski valon hallintaan käytettävään siltaan (eng. bridge), jonka avulla tutkijat onnistuivat murtautumaan myös muihin verkon laitteisiin hyödyntäen lisäksi ZigBee Light Link Touchlinkissä havaittua haavoittuvuutta. Siinä missä ZigBeen kommunikointiprotokolla avusti madon leviämistä langattomasti verkon IoT-laitteiden välillä, oli Zigbeen laitevian vuoksi

mahdollista hyödyntää standardin mukaista lähetintä kohdelaitteen tehdasasetusten palauttamiseen jopa 400 metrin päästä. ”Tehdasasetusten jälkeen kohteelle on mahdollista lähettää lisää komentoja, mitkä mahdollistavat laitteen täydellisen hallinnan.” (Paasonen, 2017) Philipsin vuonna 2020 julkaistussa päivityksessä tietoturva-aukko korjattiin. (Myllyaho, 2020)

Taulukossa 1 on vertailtu muutamia IoT-standardeja, niiden ominaisuuksia ja heikkouksia. Huomionarvoisena nostettakoon viimeisenä mainittu Matter, joka uusimpana tulokkaana on kehitetty vastaamaan tarpeeseen luoda yhtenäisyyttä IoT-laitteiden luomaan verkostoon eri valmistajien välille ja näin osaltaan lisäämään verkkojen turvallisuutta.

Taulukko 1. IoT-standardien ominaisuuksia ja heikkouksia.

Standardi	**Ominaisuudet**	**Heikkoudet**	**Salaus**
Zigbee	- luo laitteiden välille mesh-verkon: verkottaa pienet ja yksinkertaiset laitteet langattomasti - verkko koostuu kolmesta pääkomponentista: koordinaattoreista (eng. co-ordinator), reitittimistä (eng. router) ja päätelaitteista (eng. end device) - lyhyt kantama - pieni virrankulutus - perustuu IEEE 802.15.4 -standardiin	- puutteellinen varmennus ja käyttäjän identiteetin todennus -> tietojenkalastelu, man in the middle -hyökkäykset (Khanji ja muut, 2019)	AES-128
Z-Wave	- muodostaa mesh-verkon	- kaikki laitteet eivät tue salausta	AES-128

	- verkko koostuu kahdesta solmupistetyypistä: ohjaimista ja asiakaslaitteista (Parikka, 2015) - lyhyt kantama - pieni virrankulutus - itsenäinen standardi	- alttiita palvelunestohyökkäyksille (Carnegie Mellon University, 2022)	
Bluetooth Low Energy (BLE)	- muodostaa mesh-verkon - asiakas-palvelin -viestintä: esim. sensori - älypuhelin - lyhyt kantama - pieni virrankulutus - osa Bluetooth 4.0 -standardia	- parinmuodostusvaiheessa mahdollisuus yhdistää haitalliseen laitteeseen oikean sijasta -> passiivinen salakuuntelu, man in the middle -hyökkäykset (Tamminen, J., 2022)	AES-128
Thread	- langaton, IPv6-pohjainen mesh-verkkoprotokolla - eri laitevalmistajat yhdistävä standardi - lyhyt ja keskipitkä kantama - pieni virrankulutus - perustuu IEEE 802.15.4 -standardiin	- vaikka kyseessä yksi uusimmista standardeista, ei itsessään edistä IoT:n tietosuojaa juurikaan (Strayer, 2020)	AES-128
LoRaWAN	- langaton LPWAN verkkoteknologia - muodostuu LoRa-päätelaitteista, -reitittimistä, taustapalvelimista ja -sovelluksista (Digita, n.d) - pitkä kantama - pieni virrankulutus	- bitinkääntöhyökkäys: puutteet viestin eheyden ja luottamuksellisuuden tarkistuksessa päätelaitteen ja sovelluspalvelimen välillä -> viestin säilymistä muuttumattomana verkon läpi ei voida varmistaa (Lommi, 2023) - ADR-huijaus: päätelaite huijataan käyttämään heikkoa lähetystehoa ja tiedonsiirtonopeutta, jolloin lähtevät viestit	AES-128

		eivät päädy reitittimelle -> hyökkääjä kaappaa ja muokkaa ADR-aloitusviestiä, tarkoitus estää kokonaan päätelaitteen lähettämät viestit (Lommi, 2023)	
Matter	- yhtenäinen avoimen lähdekoodin standardi -> pyrkii vähentämään järjestelmien monimutkaisuutta (Gustafsson, 2023) - varmistaa, että kaikki laitteet voivat olla yhteydessä toisiinsa Bluetoothin tai Wi-Fi-yhteyden kautta, asennusvaiheessa käytössä Bluetooth Low Energy (Gustafsson, 2023) - käyttää Wi-Fi- ja Thread-protokollien yhdistelmää langattomaan viestintään - perustuu IEEE 802.15.4 -standardiin ja IPv6-yhteyksiin	- mahdolliset haasteet laitteiden yhteensopivuudessa	AES-128 AES CBC -128

3.2 Matter

Matter on yli 280 yrityksen kehittämä, avoimen lähdekoodin älykotistandardi, jonka kehitys aloitettiin vuonna 2019 nimellä Project CHIP (Connected Home over IP). Kehittäjäyritysten joukossa oli suuryrityksiä kuten Amazon, Apple ja Google. (Nordic Semiconductor, n.d.) Standardi on verraten uusi, sillä viralliseen käyttöön se julkaistiin vuonna 2022. (CSA, n.d.)

3.2.1 Miksi Matter kehitettiin?

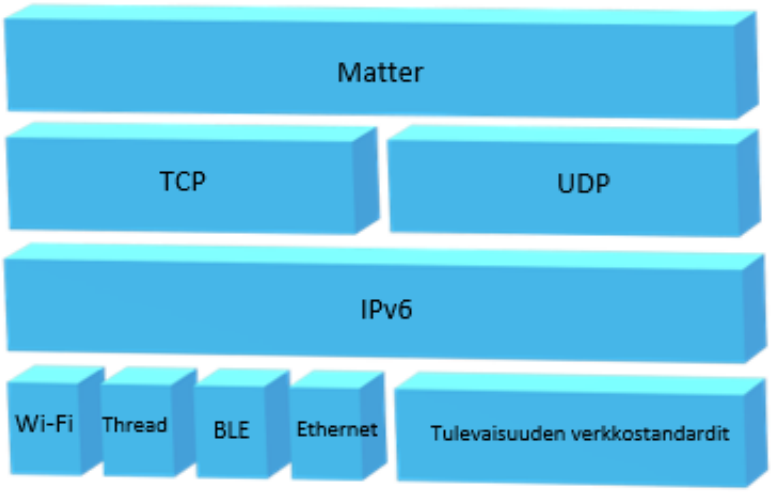
Matter-standardi kehitettiin tukemaan eri valmistajien IoT-laitteiden keskinäistä viestintää ja yksinkertaistamaan niillä luodun verkon ylläpitoa. Aiemmin eri valmistajien laitteita ei ollut suunniteltu yhdistettäväksi keskenään IoT-verkkoa rakennettaessa ja laitteet vaativat kukin oman valmistajansa hallintasovelluksen. Koska älykodissa voi olla jopa useita kymmeniä IoT-laitteita, se ei ollut kovin käytännöllistä. Yhtenä ratkaisuna ajateltiin useita protokollia tukevien laitteiden kehittämistä, mutta sen todettiin nostavan kustannuksia ja pidentävän kehitysprosessia. Näiden laitteiden haasteena nähtiin myös, että ne ”voivat yhdistää älykotien automaatiosaarekkeet vain osittain, sillä eri protokollissa käytetään erilaisia lähestymistapoja siihen, miten käyttäjien tietoturva ja yksityisyys varmistetaan, mikä vaikeuttaa entisestään suunnittelua ja toteutusta.” (Shepard, 2022)

Kuluttajan ei siis enää tarvitse keskittyä ostamaan saman valmistajan laitteita, hänen tulee ainoastaan varmistaa laitteen sisältävän Matter-tuen. Matterilla ei ole omaa sovellusta tai digitaalista avustajaa, vaan se varmistaa laitteiden yhteydenpidon Bluetoothin tai Wi-Fi-yhteyden kautta. (Gustafsson, 2023) Matterin tavoitteena on luoda yhteen toimivampi ja turvallisempi älykodin ekosysteemi määrittelemällä yhteinen kieli ja protokolla laitteiden väliseen kommunikaatioon. (CSA, n.d.)

3.2.2 Sijainti TCP/IP-protokollapinossa

Kuvassa 3 Matterin sijoittuminen TCP/IP-protokollapinoon, standardi asettuu kuljetuskerroksen ja sovelluskerroksen väliin. Edellisessä kappaleessa mainittu yhteinen kieli on verkkokerroksen IPv6, jonka avulla Matter kommunikoi laitteiden kanssa ilman kääntäjiä. Verkkokerrokseen Matter on yhteydessä kuljetuskerroksen kautta. (Silicon Labs, n.d.)

Bluetoothin ja Wi-Fi:n lisäksi Matter käyttää Ethernetia sekä Thread-standardia laitteiden väliseen viestintään. Käyttöönotossa se hyödyntää Bluetooth Low Energya (BLE): jotta verkkoon voidaan lisätä laitteita, tulee Threadiin pohjautuvien laitteiden tukea BLE:a. Wi-Fi-yhteyttä voidaan käyttää laitteissa, jotka ovat sen kattamalla alueella. (Nordic Semiconductor, n.d.)



Kuva 3. Matter TCP/IP-protokollapinossa.

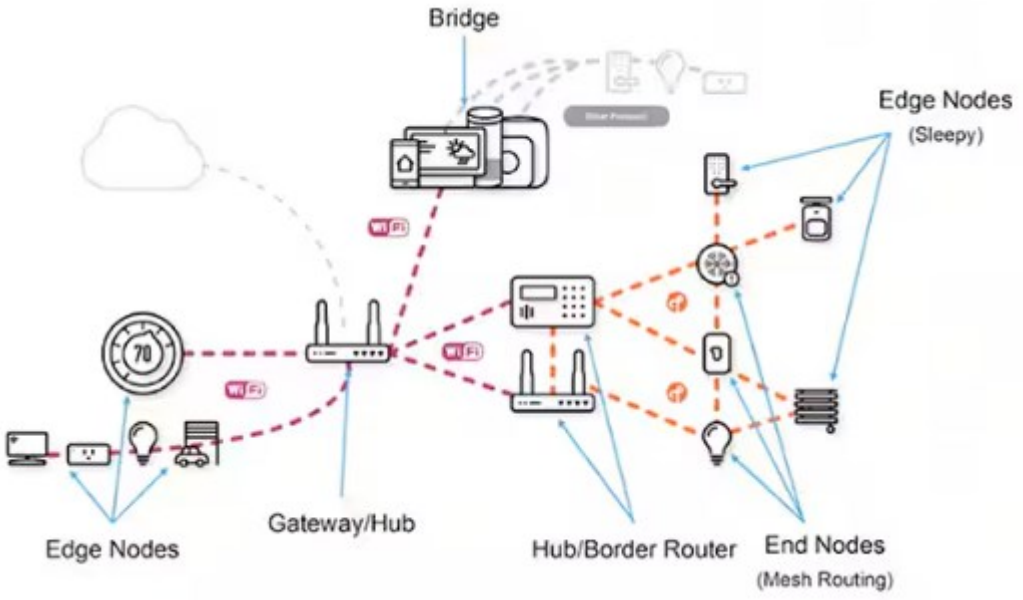
3.2.3 Salaus

Uuden standardin kehityksessä keskiössä on tietoturva, etenkin nykypäivänä, kun alalla on jo kokemusta IoT-laitteisiin ja -verkkoihin kohdistuvista uhista. Jeff Shepard (2022) kertoo Matterin huolehtivan siitä varmistamalla viestien luottamuksellisuuden ja tarkkuuden sekä todentamalla tietolähteet todennuskoodin ja salauksen yhdistelmällä. Matter käyttää AES 128 (Advanced Encryption Standard) -salausstandardin mukaista CBC (Cipher Block Chaining) -viestintodennuskoodia (CCM) tietoturvan varmistamiseen. Lisäksi se käyttää syvän suojauksen periaatetta sopivimman tietoturvan ja yksityisyystason tarjoamiseen yksittäisille laitteille.

3.2.4 Rakenne

Matter sisältää loppusolmuja kuten toimilaitteita (esimerkiksi älyvalot, -lukot), reunasolmuja erilaisten toimintojen kuten älyvalaistuksen ja älylukkojen säätimiä varten, yhdyskäytäviä, siltoja ja reunareitittimiä (**Kuva 4**). Yhdyskäytävät, joita voidaan kutsua myös ohjaimiksi, huolehtivat internetyhteydestä. Laitteiden on mahdollista käyttää viestintäominaisuuksiaan ja -toimintojaan kuten pilviyhteyksiä ja kaukosäätimiä, myös laitteen ollessa osa Matter-verkkoa. (Shepard, 2022) Sillat eli bridget yhdistävät Matter-verkot läheisiin langattomiin verkkoihin. Bridgen avulla myös laitteet, jotka eivät tue Matteria voivat toimia yhdessä Matter-verkon kanssa. Verkkorakenteeseen on mahdollista lisätä myös standardin kanssa yhteensopimattomia solmuja sekä verkkoja, ja bridgeja hyödyntäen niiden käyttöönotto nopeutuu. (Shepard, 2022)

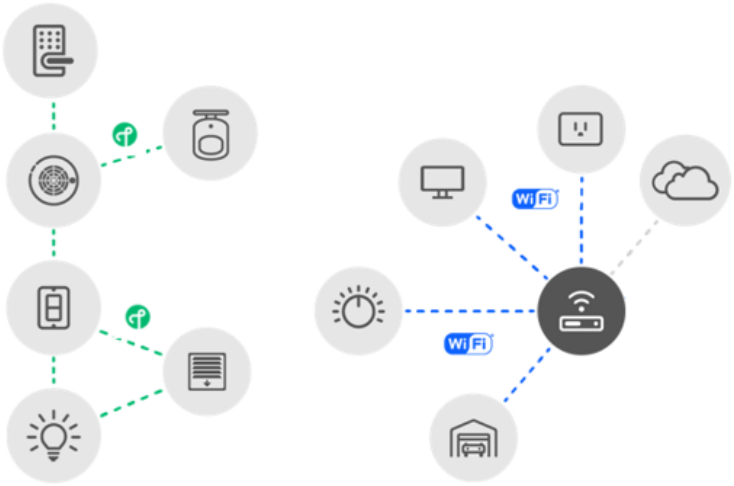
Reunareitittimien tehtävä on yhdistää Thread-verkot sekä -laitteet Matter-verkkoon ja joissain tapauksissa tarjota rajapinta älykotien hallintalaitteita varten. Reititin toimii siis siltana kahden verkon välillä. (Shepard, 2022)



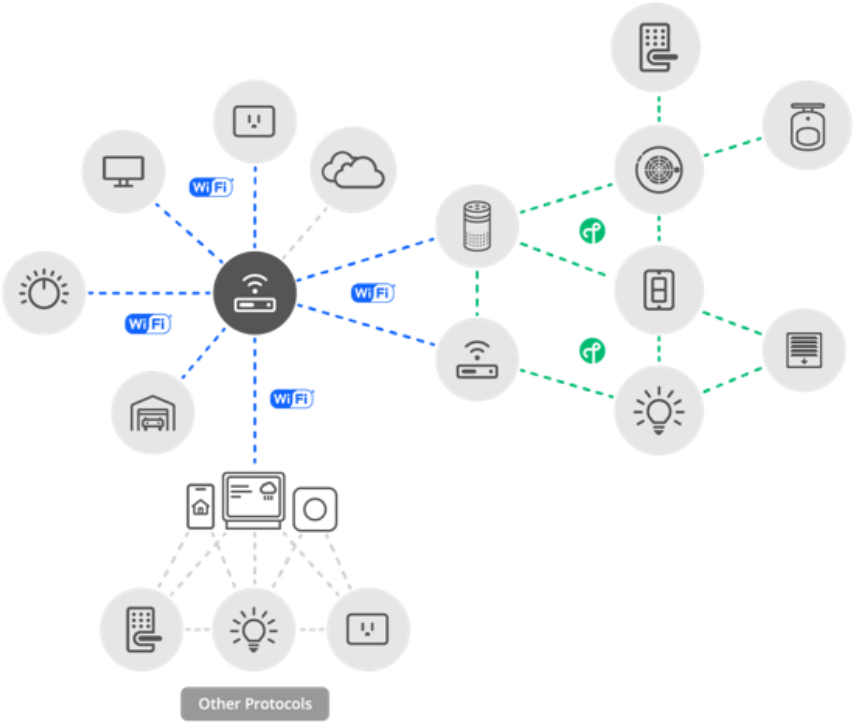
Kuva 4. Matter koostuu loppusolmuista, reunasolmuista, yhdyskäytävistä, silloista ja reunareitittimistä. (Shepard, 2022)

3.2.5 Topologia

Matter käyttää kahdenlaista verkkotopologiaa: yksittäistä (eng. single network topology) ja yleisempää tähtiverkkoa (eng. star network topology). Kuvassa 5 kaikki Matter-laitteet on kytketty samaan loogiseen verkkoon eli kyseessä on yksittäinen verkkotopologia. Nimensä mukaisesti Matter toimii siinä vain yhden, esimerkiksi Wi-Fi-verkon, kautta. Kuvassa 6 tähtiverkkotopologia, jossa keskitinverkko (eng. hub network) liittää yhteen useita oheisverkkoja reunareitittimien kautta.



Kuva 5. Matterin käyttäessä yksittäistä verkkotopologiaa laitteet on kytketty samaan loogiseen verkkoon. (Silicon Labs, n.d.)

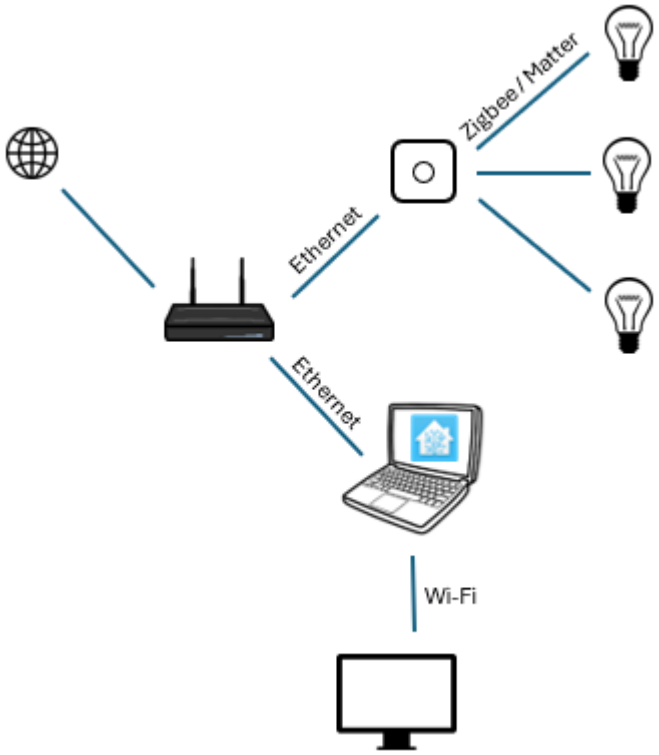


Kuva 6. Tähtitopologiaa käyttävässä Matterissa keskitinverkko liittää yhteen useita oheisverkkoja reunareitittimien kautta. (Silicon Labs, n.d.)

4 TOTEUTETTU KOTIAUTOMAATIOJÄRJESTELMÄ

Kotiautomaatiojärjestelmän komponentteina käytettiin suurimmaksi osaksi Philips Hue -valaisimia ja muita laitteita, mutta järjestelmän osiksi asennettiin myös WiZ -polttimoita, Aqara-liiketunnistin sekä Sonoff-ovi-/ikkunasensori. Kotiautomaatiojärjestelmän konfiguraatio sekä ohjaus tapahtui Home Assistant -ohjelmiston kautta, joka asennettiin erilliselle palvelintietokoneelle. Kuvassa 7 on esitetty rakennetun järjestelmän verkkotopologia: palvelimena toimii kannettava tietokone (kuvassa keskellä), joka on yhdistetty reitittimeen Ethernetin kautta. Reitittimeen on yhdistetty Ethernetin avulla myös ”hubina” toimiva Philips Hue Bridge, johon verkon IoT-komponentit, kuten valaisimet, yhdistettiin. Palvelintietokoneen porttiin numero 8123 on liitetty tietokone Home Assistantin ohjausta varten.

Työ tehdään ÄlyTech-yritykselle, joka on tekoälyratkaisuihin erikoistunut pienyritys. ÄlyTech tuottaa yrityksille chatbotteja, prosessien automaatioratkaisuja, tekoälysovelluksia sekä data-analyyseja. Toimialansa vuoksi ÄlyTechillä on kiinnostus sekä tarve selvittää mahdollisuuksia työskentely-ympäristönsä optimoimiseksi kotiautomaation mahdollisuuksia hyödyntäen.



Kuva 7. Toteutetun kotiautomaatiojärjestelmän verkkotopologia.

4.1 Haavoittuvuudet ja riskit

Kotiautomaatiojärjestelmää rakennettaessa on otettava huomioon tietoturva ja sitä uhkaavat tekijät, jotta niihin osataan varautua ja minimoida riskit. Kuvan 2 taulukossa on kuvattu älykotiympäristön keskeisimmät haavoittuvuudet ja niiden aiheuttamat riskit. Arviot perustuvat Alina Kyrölän (2021) kandidaatintutkielmassaan tekemään tutkimukseen.

Suurimpina uhkina nähdään luvaton pääsy sekä asiantuntemuksen puute. Ulkopuolisen pääsy verkkoon johtuu usein heikosta salasanasta tai tunnistautumisesta. Tunkeutuja voi aiheuttaa suurtakin vahinkoa päästessään käsiksi laitteiden keräämään dataan sekä asetuksiin ja altistamalla ympäristön erilaisille hyökkäyksille ja haittaohjelmille. Järjestelmän ylläpitäjän asiantuntemuksen puute on inhimillistä tietämättömyyttä: asioihin, joiden olemassaolosta ei tiedä, on hankala varautua.

Jokainen ei voi olla alan asiantuntija, mutta tällöin tulisi kääntyä ammattilaisen puoleen. Asiantuntemuksen puutteesta johtuen esimerkiksi laitteiden tehdasasetuksissa määriteltyä salasanaa ei huomata vaihtaa ja näin altistetaan verkko ulkopuolisille tunkeutujille ja kyberhyökkäyksille, joiden tapahtumista ei välttämättä edes huomata. Taulukossa neljäntenä mainittu fyysinen turvallisuus saattaa myös unohtua kokemattomalta tekijältä: helposti saavutettavan laitteen läheisyyteen muistilapulle kirjoitettu salasana luo ulkopuoliselle mahdollisuuden luvattoman pääsyn hyödyntämiseen.

Kolmantena mainitaan epävarmat rajapinnat ja rajapintapalvelut. Kyrölä kuvaa haavoittuvuutta seuraavasti:

> Järjestelmän taustalla saattaa pyöriä internetille altistuneita tarpeettomia, tai epävarmoja rajapintapalveluita samalla vaarantaen IoT-laitteen tai järjestelmän luotettavuuden, yhtenäisyyden sekä tiedon saavutettavuuden. Laitteen ulkopuolella olevassa ekosysteemissä saattaa myös esiintyä turvattomia verkko-, taustajärjestelmän API-, pilvi, tai mobiilirajapintoja. (Kyrölä, 2021, s. 16–17)

Riskinä on tiedon vuotaminen, joka altistaa järjestelmän luvattomalle pääsylle ja sen luomille uhille.

IoT-laitteita on saatavilla edulliseen hintaan, mikä mahdollistaa niiden saavutettavuuden yhä useammalle kuluttajalle. Valmistajat eivät kuitenkaan tarjoa säännöllisiä ohjelmistopäivityksiä laitteilleen, mikä sysää vastuuta verkon turvallisuuspäivityksien ajantasaisuudesta sen ylläpitäjälle. Tässä usein törmätään jälleen asiantuntemuksen puutteeseen, sillä päivittämättömät laitteet luovat suuren riskin kyberhyökkäykselle. Myös laitteiden moninaisuus eli erilaiset liitäntäteknologiat, sovellukset sekä palvelumallit ja niiden tietoverkkostandardien yhdistäminen vaatii ylläpitäjältään asiantuntemusta. Taulukossa tätä on kuvattu järjestelmien heterogeenisyydeksi, joka heikosti hallittuna altistaa esimerkiksi tietovuodoille. Tietojen pääsy vääriin käsiin liittyy myös alimmaksi sijoitettuun, melko yleisenä riskinä pidettyyn tietosuojaan ja yksityisyyteen. Jokainen verkkoon liitetty laite luo uhan

tietovuodolle ja tietojen väärinkäytölle. Siksi riittävä ja päivittyvä asiantuntemus on avain jokaisen taulukossa mainitun riskin pienentämiselle. (Kyrölä, 2021)

4 = kriittinen
3 = suuri
2 = kohtalainen
1 = matala

	haavoittuvuuden todennnäköisyys	Riskin toteutumisen mahdollisuus		
		Laite tai Järjestelmä	Informaatio	Henkilö-turvallisuus
Luvaton pääsy	4	Välitön	Välitön	Välitön
Asiantuntemuksen puute	4	Välitön	Välillinen	Välillinen
Epävarmat rajapinnat ja rajapintapalvelut	3	Välillinen	Välitön	Välillinen
Fyysinen turvallisuus	2	Välitön	Välitön	Välitön
Epävarmat ohjelmistot ja puutteelliset tietoturva-asetukset	2-3	Välitön	Välitön	Välillinen
Järjestelmien heterogeenisyys	4	Välillinen	Välillinen	Ei huomattavaa riskiä
Tietosuoja ja yksityisyys	3	Ei huomattavaa riskiä	Välitön	Ei huomattavaa riskiä

Kuva 8. Älykotiympäristön keskeisimmät haavoittuvuudet ja niiden aiheuttamat riskit. (Kyrölä, 2021, s. 15)

4.2 Home Assistant

Home Assistant (HA) on avoimen lähdekoodin ohjelmisto, jonka kehityksen aloitti belgialainen Paulus Schoutsen vuonna 2013. (Nabu Casa, n.d.) Ohjelmisto on suunniteltu kotiautomaation hallintaan: se kokoaa verkon komponentit kuten älyvalot, turvalaitteet sekä termostaatit yhteen käyttöliittymään, josta käyttäjän on niitä helppo hallita selainversion tai mobiilisovelluksen kautta. HA korvaa siis valmistajien omat sovellukset ja yhdistää eri valmistajien laitteet yhdelle alustalle. Ohjelmisto tukee useimpia protokollia sekä laitevalmistajia. Viimeisin versio 2024.3.3

on julkaistu 12.4.2024. (Home Assistant, n.d.a) HA voidaan integroida kotiverkkoon monin eri tavoin, esimerkiksi Wi-Fi-yhteyden, virtuaalikoneen tai erillisen palvelinkoneen kautta.

Home Assistant valittiin käytettäväksi työssä sen laajan laitetuen sekä avoimen lähdekoodin vuoksi. Jälkimmäisen ansiosta sitä päivitetään ahkerasti ja sen parissa toimii aktiivinen yhteisö, joten tukea on tarvittaessa saatavilla. Työn toteutusta varten HA asennettiin palvelimena toimivalle tietokoneelle, joka konfiguroitiin käyttämään sisäverkkoa.

4.2.1 Tietoturva

Home Assistant on paikallinen hallintaratkaisu: se toimii kotiverkossa eikä se tarvitse pilvipalveluita tai internetyhteyttä. Mikäli etäkäyttöominaisuudelle on tarve, ohjelmistoa on mahdollista käyttää HA:n oman Nabu Casa -pilvipalvelun tai eri DNS-palveluiden avulla, tällöin internetyhteys on välttämätön. (Jussila, 2023) On kuitenkin kannattavaa punnita etäyhteyden tarpeellisuutta verrattuna tietoturvariskeihin: käyttäjän päästessä käsiksi järjestelmään kodin ulkopuolelta, on siihen mahdollisuus myös hyökkääjällä. HA pyrkii huolehtimaan tietoturvasta ja käyttäjän yksityisyyden säilymisestä myös sisäänrakennetuin keinoin kuten Docker-moottorin avulla: ”Docker-konteinerin turvallisuus perustuu muun muassa hyökkäyspinta-alan pienentämiseen, tapaan kommunikoida Linux-ytimen kanssa ja verkon osioimiseen dockerin sisällä eri kontainerien kesken.” (Tuhkanen, 2022) Konteinerit eli kontit voivat olla yhteydessä toisiinsa, mutta ovat myös tehokas tapa suojata järjestelmää jakamalla se osiin, jolloin hyökkääjä ei pääse heti käsiksi kaikkeen sisältöön.

4.2.2 Asennus

Home Assistantin asennus tehtiin seuraamalla HA:n kotisivun ohjeita. Järjestelmän haluttiin käynnistyvän muistitikulta palvelintietokoneen käynnistämisen yhteydessä, joten muistitikku ”flashattiin” BalenaEtcher-ohjelmalla, jotta siitä saatiin

niin sanottu boottaava muistitikku. Tikku sekä verkkopiuha asetettiin palvelintietokoneeseen ja käynnistettiin kone, jolloin HA-palvelin käynnistyi itsestään. Home Assistantia käytetään toisen laitteen selaimella tai puhelinsovelluksella. Ensimmäisellä kerralla luotiin käyttäjänimi sekä salasana. Ohjelmassa on mahdollista luoda useita profiileja yhdelle käyttäjätunnukselle. Tämä lisää tietoturvaa, kun käyttäjille voidaan antaa rajatut käyttöoikeudet.

Opinnäytetyössä keskitytään laitteiden liittämiseen verkkoon, joten Home Assistantin kokonaisvaltaiset käyttöohjeet ovat aiheen ulkopuolella.

4.2.3 Matter-palvelin

Matter-tuettujen laitteiden käyttöönottoa varten oli Home Assistantiin asennettava lisäosa, Matter-palvelin. Kuten aiemmin todettiin, HA:n arkkitehtuuri perustuu kontteihin, jotka kukin voivat sisältää esimerkiksi yhden palvelun. Koska kyseessä on lisäosa, ei Matter-palvelimelle ole valmiiksi omaa konttia, joten sellainen luotiin.

4.3 Philips Hue

Philips Hue on Philipsin vuonna 2012 julkaisema Zigbee-protokollaan perustuva älyvalaisintuotesarja sekä automaatiojärjestelmä. Tuoteperhe sisältää valikoiman moneen käyttötarkoitukseen sopivia LED-valaisimia sekä lisälaitteita, kuten valokatkaisimia ja liiketunnistimia. Komponenttien tueksi Philips on kehittänyt ohjaussovelluksia: Hue-sovellus kaikkien Philips Hue -valojen ohjaukseen, Hue Sync -työpöytäsovellus valojen synkronoimiseksi tietokoneen näytön ja Hue Sync TV -sovellus valojen yhdistämiseksi television sisällön kanssa. Komponentit ovat yhteydessä palvelimeen ZigBee-yhteydellä. Philips Hue tukee Matter-standardia. (Philips Hue, n.d.f)

Lisäksi käytössä on Hue Bridge, joka toimii järjestelmän komentokeskuksena sekä Tap dial switch - ja Dimmer switch -kytkimet valojen ohjaukseen eri huoneissa.

4.3.1 Hue Bridge

Hue Bridgen (**Kuva 8**) avulla järjestelmään voi liittää tarvittaessa jopa 50 valaisinta sekä lisävarustetta ja etäohjata niitä internet-yhteyden avulla. Asennus tapahtuu kytkemällä laite virtalähteeseen, yhdistämällä se reitittimeen ja noudattamalla Philips Hue -sovelluksen ohjeita. (Philips Hue, n.d.a) Tässä opinnäytetyössä keskitytään Home Assistantiin, joten Philips:n sovellukset jäävät pienemmälle huomiolle.

Laite muistaa määritetyt automaatiot ja mahdollistaa lisävarusteiden räätälöinnin. Se myös huolehtii järjestelmän päivityksistä. (Philips Hue, n.d.a)

Kuva 9. Philips Hue Bridge mahdollistaa järjestelmän kasvattamisen jopa 50 valaisimen ja lisävarusteen kokoiseksi sekä etäohjauksen. (Philips Hue, n.d.a)

4.3.2 Tap dial switch - ja Dimmer switch -kytkimet

Kytkimet (**Kuva 9, Kuva 10**) on suunniteltu helpottamaan usean huoneen tai alueen valojen ohjausta yhdestä paikasta. Kukin kytkimien painikkeista voidaan konfiguroida yhden alueen hallintaan. Tässä hallinnalla tarkoitetaan valaistuksen kirkastusta, himmennystä ja kytkemistä päälle sekä pois. Kytkimiä voi käyttää valokatkaisijan tapaan kiinnittämällä taustalevy seinään, jolloin kytkin tarttuu siihen

magneetilla, tai kaukosäätimenä irrottamalla kytkin magneetista. Laite on langaton ja toimii paristoilla. Laitteen perusasetuksia voi käyttää Philips Hue -järjestelmän kanssa ilman lisäosia, mutta mukautettujen asetusten käyttö vaatii Hue Bridgen. (Philips Hue, n.d.b)

Kuva 10. Tap dial switch -kytkimellä voi kirkastaa, himmentää ja kytkeä päälle sekä pois usean huoneen valoja yhdestä paikasta. (Philips Hue, n.d.b)

Kuva 11. Dimmer switch -kytkin toimii kuten Tap dial switch. Malliltaan se on enemmän kuin totuttu kaukosäädin.

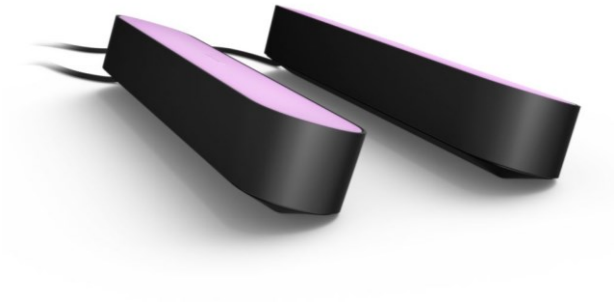
4.3.3 Älypolttimo

Lämpöisestä valkoisesta viileään päivänvalon sävyyn säädettävissä olevaa älypolttimoa (**Kuva 11**) ohjataan Bluetoothin tai Hue Bridgen avulla. Valo on kirkkaimmillaan 806 lumenia. E27-kanta mahdollistaa sen asettamisen yleisimpiin valaisinmalleihin.

Kuva 12. Lämpöisestä viileään valkoiseen valoa tarjoavan Philips Hue -älypolttimon voi asettaa useimpiin valaisinmalleihin sen E27-kannan ansiosta. (Philips Hue, n.d.e)

4.3.4 Play-valopalkki

Kuvan 12 Play-valopalkit kiinnitetään vaaka- tai pystyasentoon esimerkiksi television taakse. Valaisimen ohjaus Hue-sovelluksella vaatii Hue Bridgen. Valopalkkien mukana tulee virtalähde, jossa on paikka kolmelle palkille. (Philips Hue, n.d.d)



Kuva 13. Play-valopalkit voi kiinnittää esimerkiksi television taakse. (Philips Hue, n.d.d)

4.3.5 Led-valonauha

Lightstrip Plus V4 -valonauha (perusosa) on 2 metriä pitkä ja tuottaa 1700 lumenin, yhden väristä valoa kerrallaan. Se on himmennettävä ja valon väri on säädettävissä (värilämpötila 2000–6500 K). Perusosaa on mahdollista pidentää 10 metrin mittaiseksi saakka. (Philips Hue, n.d.c) Kuvassa 13 valonauha palaa vaaleanpunaisena.

Kuva 14. Lightstrip Plus V4 -valonauhan valoa voi himmentää, väriä muuttaa ja nauhan pituutta kasvattaa 10 metrin mittaiseksi. (Philips Hue, n.d.c)

4.4 WiZ

WiZ on vuonna 2017 toimintansa aloittanut älykomponenttivalmistaja, joka tarjoaa oman ratkaisunsa kotiautomaatiojärjestelmälle valaisimineen, oheistarvikkeineen ja ohjaussovelluksineen. Järjestelmän laitteet kommunikoivat Wi-Fi-protokollan avulla. Tuotteita on mahdollista yhdistää muiden valmistajien komponenttien kanssa kuten tässä tapauksessa Philipsin ja Aqaran. WiZ-laitteista kuitenkin vasta valaisimet ja älypistokkeet tukevat Matter-standardia. WiZ tarjoaa oman sovelluksen järjestelmän ohjaukseen, mutta laitteet ovat myös integroitavissa useimpiin älykotialustoihin. (Wiz, n.d.b)

4.4.1 Led-polttimo

Led-polttimo imitoi kynttilän liekkiä muotokieleltään (**Kuva 14**) ja valkoisen valon sävymahdollisuuksiltaan. Polttimo on kirkkaimmillaan 470 lumenia ja siinä on E14-kanta. (Wiz, n.d.a)

Kuva 15. Wizin led-polttimo muistuttaa kynttilän liekkiä muodoltaan sekä valon sävyn säätömahdollisuuksiltaan. (Wiz, n.d.a)

4.5 Aqara

Älykotijärjestelmiin erikoistunut Aqara-brändi on perustettu vuonna 2014. Se tarjoaa Zigbee-protokollaan perustuvia älylaitteita kuten valaisimia, liiketunnistimia ja lukkoja. Laitteet ovat integroitavissa useimpiin älykotialustoihin, mutta Aqara tarjoaa lisäksi oman sovelluksen laitehallintaa varten. Muiden ohella myös Aqara tukee Matter-standardia. (Aqara, n.d.a)

4.5.1 Liiketunnistin

Aqaran P1-liiketunnistin havaitsee liikkeen 170 asteen leveydeltä 2 metrin etäisyydellä ja 150 asteen leveydeltä 7 metrin etäisyydellä laitteesta. Havainnointialuetta ja syttyvän valon palamisaikaa voi säätää tarpeen mukaan. Valon voi asettaa syttymään myös ympäristön valoisuuden mukaan: ”jos valoisuus on alle 30 lumenia ja liikettä havaitaan, sytytä valo.” Kuvassa 15 nähdään myös laitteen taittuva jalka, joka mahdollistaa asennuksen monenlaisiin kohteisiin. (Aqara, n.d.b)

Kuva 16. P1-liiketunnistimen voi asettaa syttymään esimerkiksi ympäristön valoisuuden mukaan. (Aqara, n.d.b)

4.6 Sonoff

Kiinalainen Sonoff on perustettu vuonna 2016. Muiden älykotilaitteiden valmistajien tapaan, sen tuotevalikoimaan kuuluu muun muassa älypistorasioita, älyvalaisimia ja erilaisia tunnistimia kuten liiketunnistimia. Laitteet perustuvat Wi-Fi- ja Zigbee-protokolliin, osa laitteista tukee Matter-standardia. Sonoff tarjoaa oman hallintasovelluksen, mutta muiden tapaan se tukee myös useimpia älykotialustoja. (Sonoff, n.d.c)

4.6.1 Ovi-/ikkunasensori

Sonoffin SNZB-04-sensori on suunniteltu ovien ja ikkunoiden turvaamiseen. Se ilmoittaa, kun ovi/ikkuna avataan tai suljetaan. (Sonoff, n.d.a) Kuvassa 16 laitteen osat: sensori sekä pienempi magneetti, jotka asennetaan vastakkain oven/ikkunan karmiin sekä oven/ikkunan reunaan taustalla olevan tarrapinnan avulla. Hälytys aktivoituu, kun osat erotetaan toisistaan. (Sonoff, n.d.b)

Kuva 17. SNZB-04-sensori havaitsee ja ilmoittaa, kun ovi tai ikkuna avataan tai suljetaan. Laitteessa on kaksi osaa: sensori ja magneetti. (Sonoff, n.d.a)

4.7 Testitapaukset

Laitteita liitettiin verkkoon sekä Matterin että Wi-Fi:n avulla, jotta vertailu oli mahdollista. Tutkittiin, kenen on mahdollista lisätä laite verkkoon: mitä laitteen lisääminen vaatii sitä yrittävältä ja kuinka varmistetaan hänen olevan siihen oikeutettu. Tarkasteltiin myös mitä tapahtuu, jos laite putoaa verkosta.

4.7.1 Laitteiden liittäminen verkkoon Matterin avulla

Kun Home Assistantiin on asennettu Matter-palvelin, laitteen voi lisätä hyödyntäen sen mukana tulevaa QR-koodia tai ID-numeroa. Tällöin HA-sovellus tulee olla asennettuna kameralla varustettuun älylaitteeseen, jotta QR-koodi voidaan skannata sovelluksen kautta. Mikäli QR-koodia ei ole, voidaan laite lisätä myös kirjoittamalla sen ID-numero sovelluksen kenttään. Testissä käytettiin QR-koodia, jonka skannauksen jälkeen laite voitiin lisätä verkon konfiguraatioon Home Assistantissa.

4.7.2 Laitteen liittäminen verkkoon ilman Matteria

Esimerkkinä käytettiin WiZ-polttimoa, joka on valmistettu ennen sen valmistajan siirtymistä Matter-tuettujen laitteiden piiriin. Asennusta varten tarvittiin valmistajan WiZ v2 -mobiilisovellus, joka ladattiin samassa Wi-Fi-verkossa olevaan älypuhelimeen. Polttimo asetettiin paikoilleen valaisimeen ja kytkettiin virta päälle/pois viisi kertaa, jolloin polttimo alkoi välkkymään. Sovellus etsi laitteita Wi-Fi-verkosta ja tunnisti polttimon. Tämän jälkeen sovellus voitiin poistaa ja siirtyä Home Assistantiin, joka löysi laitteen automaattisesti. Laite löytyi, koska se oli yhdistetty samaan verkkoon kuin HA.

4.7.3 Laitteen liittäminen verkkoon ja laitteen hallinta – satunnainen käyttäjä

Uuden laitteen liittäminen verkkoon onnistuu vain samassa Wi-Fi-verkossa olevalta käyttäjältä, jolla on pääsy Home Assistant-järjestelmään. Verkkoon päässeeltä järjestelmää suojaa HA:n salasana, jonka on siis syytä olla korkeatasoinen.

Toinen skenaario on ulkopuolisen käyttäjän murtautuminen HA:n Wi-Fi-verkon ulkopuolelta. Tämä testattiin pyrkimällä kirjautumaan Home Assistantiin toisen verkon alueella. Yritys epäonnistui jo ennen kirjautumisyritystä: selain ilmoittaa, ettei sivustoon saada yhteyttä. Tämä johtui siitä, että yritys tapahtui Wi-Fi-verkon ulkopuolella.

4.7.4 Laitteen putoaminen verkosta

Laitteen putoamista verkosta testattiin sammuttamalla valaisin perinteisestä seinäkatkaisijasta Home Assistantin sijaan. Kyseistä valoa ei tällöin pysty ohjaamaan Home Assistantissa. Laite saadaan takaisin verkkoon palauttamalla seinäkatkaisijan asento alkuperäiseen. Vaikka yhteys laitteeseen siis katkeaisi väliaikaisesti, ei sen asennusta Philips Hue Bridgen ansiosta tarvitse aloittaa alusta.

5 OMA POHDINTA

Esineiden internet pyrkii tuomaan tavallisille käyttäjille lisäarvoa luomalla mahdollisuuksia kodin toimintojen, kuten valaistuksen, automatisointiin. IoT-komponentteja on helposti kuluttajien saatavilla elektroniikkamyymälöissä ja esimerkiksi Apple tarjoaa laitteisiinsa valmiiksi asennettuna HomeKit-kotiautomaatiosovelluksen. Näin ollen voisi ajatella, että kotiautomaatiojärjestelmän luominen on kelle tahansa erittäin helppoa. Teoriassa tämä saattaakin olla totta, mutta käännettäessä katse tietoturvaan, asia ei ole aivan niin. Kuten tämän opinnäytetyön tutkimuksessa selvitettiin, verkon suurimmat tietoturvauhat vaanivat juuri amatööriasentajia.

Home Assistant -kotiautomaatio-ohjelmisto (HA) on ilmainen, se tukee laajasti eri valmistajien laitteita ja sen käytöstä löytyy aktiivisen käyttäjäyhteisön ansiosta paljon ohjeita sekä tietoa, joten se on kuluttajalle helppo valinta ohjausjärjestelmäksi. Sen käyttöönottoon on useita eri tapoja, joista kuluttajalle mahdollisesti helpoin on yhdistää se kotiverkkoon langattomasti Wi-Fi:n avulla. Tässä työssä luodun HA-palvelimen käyttöönotto vaati erillisen laitteen ja muistitikun lisäksi useamman työvaiheen, joiden suorittaminen ei välttämättä ole kuluttajalle se miellyttävin reitti. Lisäksi se vaatii enemmän aiheeseen perehtymistä ja selvitystyötä alkaen muistitikun ”flashaus”-operaatiosta. HA:n käyttöliittymä on käyttäjäystävällinen, joten laitteiden konfigurointi on yksinkertaista. Automaatioiden luomisessa helpottaa, mikäli kuluttajalla on edes hieman ymmärrystä ohjelmointikielten logiikasta, sillä automaatiot perustuvat if-else-rakenteisiin. Home Assistantista saa irti juuri niin paljon kuin haluaa, mutta mahdollisuudet korreloivat kuluttajan oman osaamisen kanssa: pienemmälläkin asiaan vihkiytymisellä on mahdollista toteuttaa kotiautomaatiojärjestelmä, mutta mitä enemmän osaamista sitä enemmän HA:n ominaisuuksista hyötyy. Tietoturvan näkökulmasta Home Assistant on turvallinen sen jatkuvien päivitysten, tietojen paikallisen tallentamisen sekä Matter-tuen vuoksi. Käyttäjän lisätessä laitteita verkkoon Matteria hyödyntäen, hän voi luottaa sen täyttävän tietoturvavaatimukset.

Laitteen liittäminen verkkoon Matterin avulla vaatii laitteelta Matter-tuen. Matter on verrattain uusi IoT-standardi, joten siitä on vain vähän tutkimusaineistoa. Sitä on kuitenkin syytä tutkia, sillä se herättää kiinnostusta, onhan sen kehityksessä ollut mukana useita yrityksiä. Matter luotiin pääasiassa yksinkertaistamaan IoT-verkkoja ja parantamaan osaltaan myös tietoturvaa. Se varmistaa viestien luottamuksellisuuden ja todentaa tietolähteet oikeiksi todennuskoodin ja salauksen yhdistelmällä, mutta ei kuitenkaan varsinaisesti ratkaise verkon tietoturvaongelmia: sen mukana ei tule esimerkiksi lisäpalomuureja tai muita konkreettisia esteitä. Yksinkertaistamisessa se osittain onnistuu helpottamalla asennustyötä vähentämällä tarvittavia työvälineitä: yhdistellessä verkkoon eri valmistajien laitteita, ei tarvitse ottaa käyttöön jokaisen valmistajan omaa sovellusta ja eri protokollia, eikä eri valmistajien bridgejä. Työssä kävi kuitenkin ilmi, ettei Home Assistantia käyttävä kuluttaja pääse aivan näin helpolla: Matter-palvelimen asennuksen lisäksi, sille tulee luoda oma kontti. Sitä ei ollut mahdollista tehdä graafisen käyttöliittymän kautta klikkailemalla, vaan se vaati ohjelmointiosaamista.

Kuluttajan on lisäksi otettava huomioon, että vaikka valmistaja ilmoittaa tukevansa Matteria, sen kaikki laitteet eivät välttämättä niin tee. Tuki voi puuttua esimerkiksi aiemman valmistuserän laitteista. Tämä osoitettiin todeksi myös tässä työssä kotiautomaatiojärjestelmää rakennettaessa: vaikka jokaisen laitteen valmistaja ilmoitti tukevansa Matteria, ei tukea löytynyt vanhimmista yksilöistä. Nämä laitteet yhdistettiin verkkoon Wi-Fin avulla.

Monet yritykset tarjoavat kehittämiään kotiautomaatiojärjestelmiä, mutta ne tukevat usein vain yrityksen omia tuotteita eikä kuluttaja pysty itse lisäämään niihin laitteita. Käyttöönotto saattaa vaatia ammattilaisen tekemään esimerkiksi kaapelointeja ja laitteiden asennuksia. Nämä ovat niin sanottuja avaimet käteen -palveluita: käyttäjä maksaa alkukustannusten lisäksi ylläpidosta, jolloin hän voi keskittyä järjestelmän käyttämiseen eikä hänen tarvitse huolehtia ylimääräisistä asioista kuten järjestelmäpäivityksistä tai ongelmien ratkomisesta. Home Assistant tarjoaa

kuluttajalle oman tuotteensa, joka on itse rakennetun järjestelmän ja avaimet käteen -palvelun välimaastosta: HA Green on laite, johon käyttäjä liittää verkko- sekä virtakaapelin ja asentaa järjestelmän haluamansa mobiilisovelluksen (esimerkiksi Home Assistant tai Apple HomeKit) avulla. Laite sisältää Z-Wave- ja Zigbee -radiot. Green on kehitetty tarpeeseen, jossa käyttäjä haluaa aloittaa älykotiprojektin nopeasti ja välttyä eri laitteiden monimutkaisilta konfiguroinneilta. (Home Assistant, n.d.b) Enemmän resursseja ja toiminnallisuuksia kaipaaville käyttäjille Home Assistant on kehittänyt Yellow:n, joka tarjoaa muiden ominaisuuksiensa lisäksi myös tuen Matterille. (Home Assistant, n.d.c) Sekä Green että Yellow huolehtivat automaattisesti uusista Home Assistantin päivityksistä, joten myös tietoturvan kannalta ne saattavat olla hyvä valinta kotiautomaatiojärjestelmän tekoa aloittelevalle. Uskoisin, että kuluttajien käyttäessä ”puolivalmiita” ratkaisuja, olisi myös paremmat mahdollisuudet välttyä Mirain kaltaisilta laajalle levinneiltä hyökkäyksiltä, kun heikosti suojattujen amatööriverkkojen määrä vähenisi. Hintatietoinen kuluttaja saattaa kuitenkin helposti todeta ennemmin säästävänsä Green-laitteen noin 120 euron hinnan ja käyttävänsä eurot esimerkiksi IoT-laitteiden hankintaan.

Yhteenvetona voisi todeta, että vaikka IoT-laitteet sekä -verkon rakennustyökalut ovat kuluttajien tavoitettavissa helpommin kuin koskaan, ei esimerkiksi kotiautomaatiojärjestelmän pystytys ole jokaiselle kuin pala kakkua. Turvallisen ja toimivan järjestelmän luominen vaatii kuluttajalta selvitystyötä ja paneutumista, toisin sanoen jonkin verran harrastuneisuutta, tai vaihtoehtoisesti ammattilaisen puoleen kääntymistä. Kuluttajan tulisi olla kiinnostunut järjestelmästään myös käyttöönoton jälkeen, jotta sen käyttäminen säilyy turvallisena. Kokematonta verkon ylläpitäjää vaanivat monet tekijät kuten palvelinestohyökkäyksiin laitteita korruptoivat madot ynnä muut ulkopuoliset uhat. Siksi yksi tärkeimmistä asioista on huolehtia verkon laitteiden ajantasaisuudesta ja päivityksistä. Oma vastuunsa tulisi olla myös laitevalmistajilla. Tulevaisuudessa on mielenkiintoista nähdä, syntyykö Home Assistantin ja muiden vastaavien alustojen avulla kootuista kuluttajalähtöisistä järjestelmistä varteenotettava kilpailija nykyisille kotiautomaatiojärjestelmiä tarjoaville yrityksille.

LÄHTEET

Aqara. (N.d.). *Aqara.* Noudettu 26.3.2024 osoitteesta https://www.aqara.com/en/about-us/brand-story/

Aqara. (N.d.). *The Aqara Motion Sensor P1.* Noudettu 26.3.2024 osoitteesta https://www.aqara.com/en/product/motion-sensor-p1/

Carnegie Mellon University: Software Engineering Institute. (7.1.2022). Silicon Labs Z-Wave chipsets contain multiple vulnerabilities. *CERT Coordination Center*. Noudettu 21.3.2024 osoitteesta https://www.kb.cert.org/vuls/id/142629

CSA. (n.d). *Matter - The Foundation for Connected Things.* Noudettu 21.3.2024 osoitteesta https://csa-iot.org/all-solutions/matter/

Digita. (n.d). *LoRaWAN-teknologia.* Noudettu 21.3.2024 osoitteesta https://www.digita.fi/etusivu/palvelut-yrityksille/digitan-iot-palvelut/lorawan-teknologia/

European Comission. (N.d.). *Europe's Internet of Things Policy*. Noudettu 19.2.2024. https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy

Fadell, T. (7.5.2022). Tony Fadell: the nest thermostat disrupted my life. *IEEE Spectrum*. Noudettu 20.3.2024 osoitteesta https://spectrum.ieee.org/nest-thermostat

Geeks for geeks. (N.d.). *Architecture of Internet of Things (IoT).* Noudettu 19.3.2024 osoitteesta https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

Gustafsson, N. (2023). *Langaton älyvalaistus pientalossa.* [opinnäytetyö, Tampereen ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2023051110128

Hagelberg, E. (2021). *Esineiden internetin pitkän kantaman verkot.* [kandidaatintyö, Tampereen yliopisto]. Trepo-julkaisuarkisto. https://urn.fi/URN:NBN:fi:tuni-202105145003

Home Assistant. (N.d.) *Awaken your home.* Noudettu 26.3.2024 osoitteesta https://www.home-assistant.io/

Home Assistant. (N.d.) *Home Assistant Green.* Noudettu 16.4.2024 osoitteesta https://www.home-assistant.io/green

Home Assistant. (N.d.) *Home Assistant Yellow.* Noudettu 16.4.2024 osoitteesta https://www.home-assistant.io/yellow

IBM. (N.d.). *What is middleware?* Noudettu 19.3.2024 osoitteesta https://www.ibm.com/topics/middleware

José, L. (16.9.2023). Unpacking IoT Architecture: Layers and Components Explained. *Device Authority.* Noudettu 19.3.2024 osoitteesta https://www.deviceauthority.com/blog/unpacking-iot-architecture-layers-and-components-explained/

Jussila, N. (2023). *Home Assistantin käyttö Raspberry Pi:llä.* [opinnäytetyö, Hämeen ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2023111529472

Juxtology. (N.d.). *IoT: Architecture.* Noudettu 19.3.2024 osoitteesta https://www.m2mology.com/iot-transformation/iot-world-forum/

Khanji, S., Iqbal, F. & Hung, P. (2019). ZigBee Security Vulnerabilities: Exploration and evaluating. *IEEE Explore.* Noudettu 21.3.2024 osoitteesta https://ieeexplore.ieee.org/document/8809115

Kyrölä, A. (2021). *IoT-laitteiden kyberturvahaavoittuvuudet älykotiympäristössä.* [kandidaatintutkielma, Jyväskylän yliopisto]. JYX-julkaisuarkisto. http://urn.fi/URN:NBN:fi:jyu-202109164881

Logistiikan maailma. (N.d.). *Esineiden internet*. Noudettu 19.2.2024 osoitteesta https://www.logistiikanmaailma.fi/logistiikka/digitalisaatio/esineiden-internet/

Lommi, J. (2023). *Lorawan-teknologian soveltuvuus kriittisen tiedon välittäjänä.* [kandidaattitutkielma, Tampereen yliopisto]. Trepo-julkaisuarkisto. https://urn.fi/URN:NBN:fi:tuni-202309198303

Myllyaho, T. (2020). *IoT-laitteet kotona ja niiden tietoturva.* [opinnäytetyö, Oulun ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2020052915236

Nabu Casa. (N.d.). *About us.* Noudettu 15.4.2024 osoitteesta https://www.nabucasa.com/about/

Nordic Semiconductor. (N.d.). *Matter Protocol.* Noudettu 21.3.2024 osoitteesta https://www.nordicsemi.com/Products/Technologies/Matter

Oracle. (N.d.). *What is IoT?* Noudettu 28.2.2024 osoitteesta https://www.oracle.com/internet-of-things/what-is-iot/

Paasonen, A. (2017). *Internet of Things – Haavoittuvuuksien verkko*. [opinnäytetyö, Kajaanin ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2017120419750

Parikka, J. (2015). *Z-wave langaton kodinohjausjärjestelmä.* [opinnäytetyö, Karelia-ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2015052610470

Philips Hue. (N.d.). *Hue Bridge.* Noudettu 26.3.2024 osoitteesta https://www.philips-hue.com/fi-fi/products/all-products/product-page/hue-bridge#overview

Philips Hue. (N.d.) *Kytkimet.* Noudettu 26.3.2024 osoitteesta https://www.philips-hue.com/fi-fi/p/hue-tap-dial-switch--kytkin/8719514440999#overview

Philips Hue. (N.d.). *Lightstrip Indoor.* Noudettu 26.3.2024 osoitteesta https://www.philips-hue.com/fi-fi/p/hue-white-and-color-ambiance-lightstrip-plus-v4--perusosa--2-metria/8718699703424

Philips Hue. (N.d.). *Play Light Bar.* Noudettu 26.3.2024 osoitteesta https://www.philips-hue.com/fi-fi/p/hue-white-and-color-ambiance-play-valopalkin-tuplapakkaus/7820230P7#overview

Philips Hue. (N.d.). *Smart bulb.* Noudettu 28.3.2024 osoitteesta https://www.philips-hue.com/en-my/p/hue-white-ambiance-a60---e27-smart-bulb---800/8718699719319

Philips Hue. (N.d.). *Viralliset Philips Hue -sovellukset.* Noudettu 26.3.2024 osoitteesta https://www.philips-hue.com/fi-fi/explore-hue/apps

Pörhölä T. S. (2017). *Internet of things - Esineiden Internet.* [opinnäytetyö, Oulun ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2017113019036

Shepard, J. (23.12.2022). How to Use Matter to Connect the Islands of Smart Home Automation. *DigiKey*. Noudettu 21.3.2024 osoitteesta https://www.digikey.co.uk/en/articles/how-to-use-matter-to-connect-the-islands-of-smart-home-automation

Silicon Labs. (N.d.). *Introduction to Matter.* https://docs.silabs.com/matter/latest/matter-fundamentals-introduction/

Simmons, A. (13.11.2022). Internet of Things (IoT) Architecture: Layers Explained. *Dgtl Infra*. Noudettu 19.3.2024 osoitteesta https://dgtlinfra.com/internet-of-things-iot-architecture/

Simmons, A. (9.1.2023). Internet of Things (IoT) Edge: Computing for Devices. *Dgtl Infra*. Noudettu 19.3.2024 osoitteesta https://dgtlinfra.com/internet-of-things-iot-edge/

Sissala, P. (2021). *Wi-fi-verkon tietoturva.* [opinnäytetyö, Vaasan ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-202105108037

Sonoff. (N.d.). *SNZB-04.* Noudettu 26.3.2024 osoitteesta https://sonoff.tech/product/gateway-and-sensors/snzb-04/

Sonoff. (N.d.). *SNZB-04 User manual V 1.0.* Noudettu 26.3.2024 osoitteesta https://sonoff.tech/wp-content/uploads/2021/03/%E8%AF%B4%E6%98%8E%E4%B9%A6-SNZB-04-V1.0-20210305.pdf

Sonoff. (N.d.). *Sonoff.* Noudettu 26.3.2024 osoitteesta https://sonoff.tech/

Strayer, K. W. (9.4.2020). Can the “Gorilla” Deliver? Assessing the Security of Google’s New “Thread” Internet of Things (IoT) Protocol. *CSIAC - Cybersecurity & Information Systems Information Analysis Center.* Noudettu

21.3.2024 osoitteesta *https://csiac.org/articles/security-of-googles-iot-protocol/*

Tamminen, J. (2022). *BLE-mobiilisovellus ilmanlaatua mittaavalle olosuhdeanturille.* [opinnäytetyö, Metropolia Ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2022110822306

Tamminen, T. (2022). *Datasta arvoa: datan hallinnan, varastoimisen ja hyödyntämisen periaatteet.* [opinnäytetyö, Tampereen ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2022051810076

Tietosuojavaltuutetun toimisto. (N.d.). *Tietosuoja.* Noudettu 20.3.2024 osoitteesta https://tietosuoja.fi/tietosuoja

Tuhkanen, T. (2022). *Kotiautomaatio ja sen tietoturva.* [opinnäytetyö, Vaasan ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2022053013037

Uppa, J. (2017). *Esineiden internet ja IoT-alustat.* [opinnäytetyö, Tampereen ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2017121320895

Vaughan-Nichols S. J. (11.1.2024). NoaBot: Another Mirai Botnet Strikes at Linux Devices. *The New Stack*. Noudettu 20.3.2024 osoitteesta https://thenewstack.io/noabot-another-mirai-botnet-strikes-at-linux-devices/

Vedenpää, V. (2019). Blade Runner -elokuva kertoi vuodesta 2019 – mitkä tulevaisuudenkuvista toteutuivat? *Yle*. Noudettu 19.2.2024 osoitteesta https://yle.fi/a/3-10578400

Väisänen, P. (20.11.2019). IIoT ja BI – näin ne tehostavat teollisuuden analytiikkaa. *Pinja Blogi*. Noudettu 28.2.2024 osoitteesta https://blog.pinja.com/fi/iiot-ja-bi-nain-ne-tehostavat-teollisuuden-analytiikkaa

WiZ. (N.d.). *Candle 40W C37 E14.* Noudettu 26.3.2024 osoitteesta https://www.wizconnected.com/en-au/p/modern-bulb-candle-40w-c37-e14/8718699787073

WiZ. (N.d.). *Lights that make your home life brighter*. Noudettu 26.3.2024 osoitteesta https://www.wizconnected.com/en-au