IoT-verkot ja palvelut Suomessa

Ammattikorkeakoulututkinnon opinnäytetyö

Riihimäki, Tietotekniikan koulutusohjelma

Kevät, 2017

Santtu Laine

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietotekniikka
HAMK Riihimäki

Tekijä Santtu Laine **Vuosi** 2018

Työn nimi IoT-verkot ja palvelut Suomessa

TIIVISTELMÄ

Opinnäytetyön tarkoitus on selvittää Internet of Thingsin kehitys ja tilanne palveluiden ja verkkojen suhteen Suomessa. Opinnäytetyössä käydään teoriatasolla läpi IoT-verkon rakennetta ja yleistasolla IoT-verkon mahdollistamia uusia palveluita. Lisäksi tutkitaan IoT:n tuomia hyötyjä eri näkökulmista Suomelle ja mitä haasteita tämän kasvavan trendin tiellä on vielä ratkaisematta.

Julkisuudessa IoT:ta ollaan hehkutettu jo monta vuotta, mikä tekee siitä kiintoisan aiheen. Tätä ilmiötä ollaan povattu seuraavaksi teolliseksi vallankumoukseksi, joka tulee muuttamaan yrityksien ja kuluttajien arjen. IoT tapahtuu tässä ja nyt, mutta vielä ei osata kertoa mihin se johtaa.

Suomessa ollaan herätty IoT:n mahdollistamaan taloudelliseen ja teknologiseen potentiaaliin ja vireillä on monia kehityshankkeita. Vain pienelle osalle Suomen yrityksistä IoT on jo normaalia arkea. Suomi kuuluu IoT:n kehityksen eturintamaan, mutta suurin osa yrityksistä panostaa siihen kuitenkin vielä maltillisesti. Opinnäytetyön aiheen laajuuden vuoksi tutkimuksessa pysytään hyvin yleisellä tasolla, eikä yksittäisiin hankkeisiin perehdytä syvällisemmin.

Avainsanat Digitalisaatio, Esineiden Internet, IoT, Teollinen Internet

Sivut 31

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information Technology
HAMK Riihimäki

Author Santtu Laine **Year** 2018

Subject IoT Networks and Services in Finland

ABSTRACT

The purpose of the thesis project was to examine the development of the Internet of Things and the situation with regard to services and networks in Finland. This thesis deals with the structure of the IoT network at a theoretical level and introduces the new services provided by the IoT network at a general level. In addition, the benefits of the IoT to Finland from different perspectives are discussed while the challenges of this growing trend still remain unresolved.

In public, IoT has been hyped for many years, which makes it a very interesting phenomenon. This phenomenon is being pushed to the next industrial revolution, which will change the everyday lives of business and consumers. IoT takes place here and now, but still no one can tell where it will lead.

In Finland, we have been awakened by the economic and technological potential of IoT and many development projects are underway. IoT is already normal everyday life for only a handful of Finnish companies. Finland belongs to the forefront in the development of IoT, but most companies are still investing in to it only moderately. Due to the scope of the subject of the thesis, the topic is examined at a very general, and individual projects have not dealt with deeper in the thesis.

Keywords Digitalization, Industrial Internet, Internet of Things, IoT

Pages 31

SISÄLLYS

1 JOHDANTO

Tässä opinnäytetyössä tarkoituksena oli tutkia digitalisaatioon kuuluvaa Internet of Things (IoT) -ilmiötä yleisellä tasolla. IoT on tällä hetkellä hyvin ajankohtainen aihe, koska tämän teknologian uuden murroksen odotetaan muuttuvan puheista teoiksi jo vuonna 2018. Esineiden internet kasvaa kiihtyvää tahtia, koska vuoden 2015 lopussa esineiden internetin tai teollisen internetin laitteita oli kytketty verkkoon jo 4,6 miljardia kappaletta ja rohkeimpien ennusteiden mukaan 2020-luvulla laitteita olisi jo 50-100 miljardia kappaletta. (Lehto 2016.)

Opinnäytetyön aihe on hyvin laaja, mutta aihetta on pyritty rajaa koskettamaan IoT-ilmiön tapahtumista Suomessa. Tavoitteena on kuvailla yleisellä tasolla mitä IoT:lla tarkoitetaan ja miten esineiden internet ja teollinen internet eroavat toisistaan. Opinnäytetyössä käydään läpi, miten IoT-verkko luodaan teoriassa, kuinka paljon IoT-verkkoja on hyödynnetty ja mitä uusia palveluita IoT voi tarjota Suomessa. Työssä käydään läpi myös IoT:n tuomia hyötyjä, uhkia, tulevaisuuden näkymiä ja sen luomia haasteita.

Tässä tutkimuksessa on käytetty tukena aiheeseen liittyvää kirjallisuutta, asiantuntijaraportteja, lehtiartikkeleita, opinnäytetöitä, yritysten internet-sivustoja ja tutkimuksia.

2 IOT:N MÄÄRITELMÄT JA KÄSITTEITÄ

Internet of Things, suomennettuna esineiden tai asioiden internet, termin on maininnut luultavasti ensimmäisenä Kevin Ashton, joka on yksi perustajista ja johtaja MIT:n Auto-ID Centerissä, esityksessään Procter & Gamblelle vuonna 1999. Ashton kuvaili IoT:n potentiaalia seuraavasti: ”Vielä tänä päivänä tietokoneet - ja täten internet - ovat suuressa osassa täysin riippuvaisia ihmisestä informaation keräämisen osalta. Melkein kaikki avoin data internetissä, jota on todella suuri määrä, on ensin kerätty ja luotu ihmisen toimesta joko kirjoittamalla, nauhoittamalla, kuvaamalla tai skannaamalla viivakoodi. Ongelmana on kuitenkin ihmisen rajoittunut ajankäyttö, huomio ja tarkkuus, jotka eivät ole niin sopivia jatkuvan datan keräämiseen esineistä. Jos meillä olisi tietokoneet, jotka tietäisivät kaiken mitä esineistä voisi tietää – käyttäisivät keräämänsä datan ilman meidän apua – me voisimme suuresti vähentää kulutusta, hävikkiä ja kustannuksia. Tietäisimme kun esineet pitäisi vaihtaa, korjata tai ovat ohittaneet parasta ennen päivänsä.” (Ashton 2009.)

IoT alkoi kasvaa trendinä kuitenkin vasta vuonna 2014 (Guinard & Trifa 2016). IoT:n yhteydessä puhutaan myös paljon teollisesta internetistä. IoT voidaan jakaa teolliseen internetiin ja esineiden internetiin. Esineiden internet jakautuu enemmän kuluttajille suunnattuihin palveluihin, pieniin langattomiin verkkoihin tai yksittäisiin laitteisiin, kun taas teollinen internet pitää sisällään laajat sensoriverkot, jotka kuuluvat yleensä keskitettyyn tuotantojärjestelmään, jossa dataa jalostetaan analysoinnilla. Tässä opinnäytetyössä pidetään IoT:ta yleisenä käsitteenä koskemaan koko ilmiötä ja painotetaan yrityksien puolta teollisella internetillä ja kuluttajan puolta esineiden internetillä.

Ei ole olemassa selvää rajaa mikä luokitellaan IoT:hen ja mikä taas ei, mutta IoT voidaan kuitenkin määritellä seuraavasti: Esineiden internet on fyysisten esineiden järjestelmä, mikä on elektronisten laitteiden havaittavissa, valvonnassa, ohjauksessa tai vuorovaikutuksessa. Lisäksi älyllä laajennetut esineet voivat kommunikoida erilaisten verkkoliitäntöjen läpi ja tarvittaessa ovat liitettävissä internetiin. Puhutaan siis älykkäistä esineistä, fyysistä objekteista, joihin on digitaalisesti lisätty yksi tai useampi seuraavista laajennuksista:

•Sensoreita (lämpötila, valo, liike)

•Aktuaattori (näyttö, ääni, moottori)

•Laskin (ajaa ohjelmia tai logiikkaa)

•Tiedonsiirtoliitäntä (langallinen tai langaton)

Älykkäät esineet yleistyvät ja levittäytyvät luoden mahdollisuuksia aivan uusille palveluille ja sovelluksille. Pieniä ja halpoja, mutta tehokkaita, tietokoneita voidaan kytkeä nykyään kaikkialle, mikä mahdollistaa digitaalisen vuorovaikutuksen fyysiseen maailmaan, ja sen monitorointiin. Näin saadaan tarkempaa paikka- ja aikatietoa halutuista kohteista kuin koskaan aikaisemmin. (Guinard & Trifa 2016, 4.)

Esineiden internetiin kuuluvien älykkäiden fyysisten objektien kirjo on hyvin laaja. Siihen voidaan luokitella yksinkertainen postipaketti, jossa on automaattinen tunnistusleima, kuten esimerkiksi viivakoodi, QR, NFC tai RFID, jonka avulla paketin matka on seurattavissa lähetyspisteestä vastaanotto pisteeseen. Kehittyneempiä ja monimutkaisempia langattomasti liitettyjä älykkäitä tuotteita voivat olla esimerkiksi turvajärjestelmä, auto, tehtaan tuotantolinja, tai talo aina kokonaiseen älykaupunkiin asti. Älykkään esineen ei kuitenkaan tarvitse kuulua suoraan internetiin, mutta esinettä laajennetaan tällöin erilaisilla verkkoliittimillä, joita voivat olla esimerkiksi Auto-ID, lyhyttaajuinen radioaalto (Bluetooth, ZigBee) tai rakennuksen oma WiFi-verkko. (Guinard & Trifa 2016, 6.)

3 IOT SUOMESSA NYT

3.1 IoT:n nykyasema Suomessa

Digitalisaatio on kehittynyt kiihtyvää tahtia 1990-luvulta eteenpäin, tuoden jatkuvasti digitaalisia laitteita osaksi meidän arkeamme. Esineiden internetiä, joka on osa digitalisaatiota, pidetään seuraavana eli kolmantena teollisena vallankumouksena. Esineiden internetin tilaa Suomessa on vaikea kuvata, koska IoT-laitteille ei ole selvää rajaa, mikä lasketaan sen joukkoon ja mikä ei. Lisäksi kuluttajille suunnatut palvelut ovat tehty niin helppokäyttöisiksi, että niitä on hankala edes tiedostaa osaksi esineiden internetiä, kuten muun muassa Fortumin käytössä olevat sähkömittarit, jotka ovat olleet hetken jo käytössä, ja asiakkaat voivat älypuhelinsovelluksella tarkkailla oman talouden sähkönkulutusta.

Teollisen internetin kehitystä eri maiden välillä voidaan vertailla erilaisilla mittareilla, jotka ovat: Teollisen internetin aikaansaama kehitys, julkistukset, uudet tuotteet, yrityskaupat ja julkisuus. Vuosina 2013-2014 mitattiin alueet tai maat, jotka ovat olleet eniten esillä termillä ”industrial internet” uutisten yhteydessä. Vertailun mukaan Suomi ei kuulu aivan kirkkaimpaan kärkeen Yhdysvaltojen ja Saksan kanssa. Suomi kuuluu kuitenkin teollisen internetin kehityksen eturintamaan yhdessä Australian, Kiinan ja Kanadan kanssa, vaikka Suomen markkina on huomattavasti pienempi. (Juhanko ym. 2015, 43.)

Suomi kuuluu IoT-kehityksen eturintamaan, koska Suomessa dataan perustuvia ja käytön mukaan laskutettavia muita kuin IT-palveluja tarjoaa 26% organisaatioista. Globaalisti vastaava luku on 21 %. Ja IoT-ratkaisuissa ollaan siirtymässä Suomessa yksittäisistä piloteista ensimmäisiin laajempiin käyttöönottoihin. (Hänninen 2017.)

Yrityksien ja organisaatioiden kehitystä esineiden internetissä voidaan kuvata portaikolla, jossa on tasot 1-5. Ensimmäisellä portaalla laite tai tuote ei ole älykäs. Toisella portaalla laitteeseen lisätään älykkäitä toimintoja, jolloin se voi tarkkailla tai mitata omaa tai ympäristönsä toimintaa ja vuorovaikuttaa siihen. Laitteeseen ei kuitenkaan saada tällä portaalla vielä yhteyttä ulkopuolelta. Kolmannella tasolla laitteella on jokin protokolla, esimerkiksi Bluetooth tai Wi-Fi, joka mahdollistaa laitteen tai tuotteen liittämisen suljettuun taustajärjestelmään. Neljännellä tasolla laitteen tai tuotteen taustajärjestelmiin on kytketty analytiikka ja jalostettu tieto ohjaa yrityksen toimintaa. Ylimmällä tasolla yritys on kehittänyt täysin uusia liiketoimintamalleja tai tapoja tuottaa palveluja. (Arrow 2015.)

IoT:lla on jo suuri asema Suomessa energia-, teollisuus- ja rakennusaloilla, koska 2/3 yrityksistä ilmoittaa, että IoT kuuluu osaksi yrityksen kehityssuunnitelmaa. Suurin osa yrityksien tuotteista ja laitteista kuuluvat jo IoT:n kehitysvaiheisiin, joissa älykäs laite tai tuote on liitetty taustajärjestelmään, tai kehittyneempään vaiheeseen, jossa taustajärjestelmään on kytketty analytiikka ja jalostettu tieto ohjaa toimintaa. Kuitenkin ylimmälle portaalle ylsi vain 8% haastatelluista yrityksistä. Lisäksi keskustelu ja päätöksenteko IoT:hen liittyvistä asioista on siirtynyt lähivuosina enemmän alaspäin yrityshierarkiassa ylimmältä johdolta asiantuntijoille. (Arrow 2017.)

3.2 **IoT-palvelut Suomessa**

Yrityksille, jotka ovat saavuttaneet IoT-portaikon tason 4, avautuu aivan uudenlaiset mahdollisuudet kehittää liiketoimintamalleja ja uusia tapoja tuottaa palveluita. Suuri älykäs laitekanta antureineen kerää todella suuren määrän dataa laitteista tai tuotteista, jota analysoidaan automaattisilla big datan tiedonhallintavälineillä. Tarkemmilla, kattavilla ja jopa reaaliaikaisilla analyyseillä yritykset voivat ohjata liiketoimintaansa oikeaan suuntaan ja tuoda lisäarvoa asiakkaiden palveluihin.

3.2.1 Uusi datapohjainen palveluliiketoiminta

Teollisuuteen voi syntyä kokonaan uusia palveluliikemalleja, kun tuotteiden valmistajien ei tarvitse enää tyytyä pelkästään tuotteiden valmistamiseen ja myyntiin. Tuote voidaan myydä palveluna, kun se on koko ajan verkossa ja dataa välittyy valmistajalle. Valmistajat voivat myös pilkkoa myytäviä palveluita, joihin voi kuulua muun muassa etäoptimointi, etähallinta ja ennakoiva huolto. Palveluliiketoiminnassa vastuu tulee siirtymään yhdeltä käyttäjältä kone- tai laitevalmistajan vastuulle. Käyttäjiä tulee monta ja toimittajan vastuulle kuuluu laitekannan tilanvalvonta ja hyödyntäminen. Aikaisemmin koneiden toiminnasta kerättiin tietoa käsin ja tietoa vaihdettiin partnereiden kanssa, mutta toimittaja pystyy nyt keräämään älykkäillä laitteilla tiedot automaattisesti kaikista laitteista ja analysoimaan datan, joka voidaan hyödyntää toiminnan parantamiseksi. Käytännössä laitevalmistaja ei enää myy valmistamaansa tuotetta, vaan tuote myydään asiakkaalle palveluna. Asiakkaan ei tarvitse tehdä suuria laiteinvestointeja, eikä asiakaspalautteita tuotteesta, koska älykäs tuote kerää toiminnastaan jatkuvasti dataa. (Collin & Saarelainen 2016, 81.) Tämä liiketoimintamalli tarvitsee kuitenkin muutosta ihmisien asenteessa tuotteiden omistamisen suhteen, mikä riippuu pitkälti tuotteesta, koska esimerkiksi auton ostaminen palveluna on todennäköisesti vielä suuri kynnys monelle asiakkaalle.

Tähän asti tietoa tuotteen laadusta ja toimintakyvystä on saatu tehtaalla ennen tuotteen asiakkaalle lähettämistä ja kun tuote tulee takaisin huoltoon, on saatu tietoa tuotteen kulumisesta. Laadunvalvonta ja tuotekehitys tulevat parantumaan, koska valmistajat saavat jatkuvasti dataa asiakkaan todellisesta käytöstä ja ominaisuuksista, joissa ilmenee kulumista. Datan avulla voidaan kehittää tuotetta ja niiden turhia ominaisuuksia voidaan poistaa, kun huomataan, ettei niille ole oikeasti käyttöä. Lisäksi dokumentaatio tulee automatisoitumaan, ennen dokumentit tehtiin manuaalisesti, mutta jatkossa tuotteen jokainen vaihe tulee dokumentoitua digitalisesti ja tuotteet voivat itse "muistaa" ja "tietää" miten, missä ja milloin ne on valmistettu. (Collin & Saarelainen 2016, 82.)

3.2.2 Etävalvonta, etähallinta, optimointi ja etäpäivitykset

Etävalvonta ja etäoptimointi ovat kuuluneet teollisuuteen jo ennestään pitkän ajan, mutta teollinen internet tuo mukanaan pilvipalvelut, big datan ja data-analytiikan. Uudet sovellukset ja palvelut mahdollistavat jo kerätyn ja reaaliaikaisen datan analysoinnin. Sensoreista kerätyn datan hyöty saadaan esille, kun älykkäät laitteet yhdistetään

samaan verkkoon ja kerätty data siirretään keskitettyyn käyttöliittymään. (Collin & Saarelainen 2016, 63.)

Laitekannan hallinta sisälsi ennen tiedot laitemääristä, kaluston koostumuksesta, kaluston sijainnista ja käytöstä. Mutta nyt etävalvonnalle avautuu reaaliaikainen näkymä kaluston tila- ja paikkatiedoista, josta näkee myös mitä laitteella tehdään parhaillaan ja lisäksi voi avata lokien historiatiedot. Etävalvontayritys voi kerätä jatkuvan datayhteyden ansiosta enemmän ja tarkempaa dataa omasta tuotteestaan, kun nähdään miten ja missä ympäristössä asiakas oikeasti käyttää laitetta. Näin voidaan valvoa, että asiakas käyttää tuotetta oikein ja voidaan reagoida tuotteen väärinkäyttöön, muun muassa puuttumalla toimintaan tai lisäämällä koulutusta laitteen käytöstä. Toisaalta voidaan todeta, että laite on viallinen ja kerätyn datan avulla voidaan nähdä, miten vika on syntynyt. Reaaliaikaisen näkymän ansiosta on mahdollista, että vika havaitaan ja korjataan etänä ohjelmistopäivityksellä jo ennen reklamaatiota. Esimerkiksi Helsingin bussiliikenne toteutti ajotavan analyysin anturidatan avulla, joka johti rauhallisempaan ajotapaan ja säästi näin polttoainekuluja ja bussin laitteistoa rasitukselta. Aikaisemmin bussikuljettajien ajotavasta saatiin tietoa vain asiakaspalautteilla. (Collin & Saarelainen 2016, 63-64.)

Etähallinnalla tuotteita tai laitteita voidaan hallita sijainnista riippumatta ja se voi olla laitteen täydellistä hallintaa tai asetusten optimointia reaaliaikaisesti tarpeen vaatiessa. Etähallintaa ja etäoptimointia on tietysti toteutettu aikaisemminkin, mutta nyt älykkäiden tuotteiden sensoreilla kerätyn datan analytiikan ansiosta voidaan saavuttaa merkittäviä hyötyjä. Ongelmat voidaan havaita ja muutokset voidaan toteuttaa reaaliajassa tai ainakin entistä nopeammin ja tarkemmin. (Collin & Saarelainen 2016, 64.)

Etähallinnan avulla voidaan laitekannan päivityksetkin ajaa etänä, joka on välttämätöntä tilanteessa, jossa verkkoon kuuluu tuhansia sensoreita. Teollisessa internetissä luonteen omaista on, että äly sijaitsee ohjelmistossa eikä raudassa kuten aikaisemmin, etäpäivityksillä voi korjata ohjelmistovirheitä ja parannella tietoturvaa. Lisäksi sensoreiden mittaavia antureita voidaan kalibroida uudelleen tai muuttaa niiden parametreja. Älykkäiden laitteiden omistajien ei pidä tyytyä vain valmistushetken ominaisuuksiin, koska ohjelmiston kehitystyötä tehdään jatkuvasti. (Collin & Saarelainen 2016, 65.)

3.2.3 Ennakoiva huoltopalvelu ja analytiikka

Ennakoivan huollon odotusarvo on teollisen internetin sovellusalueista suurin, koska sen odotetaan nostavan eniten tuottavuutta paremmalla laitteiden käyttöasteella, harvemmilla käyttökatkoksilla ja lyhyemmillä suunnitelluilla huoltokatkoilla. Ennakoivan huollon hyödyn mahdollisuudet vaikuttavat suoraan yrityksien kannattavuuteen. Ennakoiva huolto vaatii käyttäjien laitteisiin vähintään etävalvonnan, mutta parempaa huoltopalvelua varten myös etänä toimiva laitteiden tai tuotteiden hallinta, optimointi ja päivitys. (Collin & Saarelainen 2016, 73.)

Ennakoivalla huollolla kestää hetken aikaa ennen kuin se voi alkaa toimia käytännössä täydellä potentiaalillaan, koska laitteiden käyttäytymistä pitää seurata pitkä aika ennen

kuin ennustuksista tulee tarkkoja. Aikaisemmin ei ole ollut resursseja valvoa käsin datassa ilmeneviä poikkeamia, mutta automaatio mahdollistaa jatkuvan tarkkailun. Vikoja ja hälytyksiä täytyy ensin syntyä, jotta analytiikalla voidaan huomata vikaa ennen ilmenevät poikkeamat laitteista, ja vasta ajan kuluessa poikkeamiin osataan reagoida ennustamalla tarkemmin vikoja. Laitteiston rikkoutumisia aiheuttavat poikkeamat voivat olla muun muassa epätavalliset tapahtumat tuotannossa, ympäristön olosuhteiden vaihtuminen, tai laitteiston virheellinen käyttötapa. Anturit keräävät datan näistä tekijöistä ja analytiikan avulla huolto saa ne tietoonsa. (Collin & Saarelainen 2016, 74.)

Laitteiston huoltoa ollaan aina pyritty ennustamaan, mutta analytiikka mahdollistaa huollolle entistä tarkemman ajoituksen vaativilla laskutekniikoilla. Huollon oikea ajoitus on iso tekijä laitteiden käyttöasteelle. Ennakoiva huolto suoritetaan tuotteen todellisen kunnon mukaan ja määräaikaishuollot voidaan jättää historiaan. Määräaikaishuolto perustui ennalta ehkäisyyn, ja huollon ajankohta määriteltiin laitteen keskimääräisen rikkoutumisen odotusarvon mukaan. Ennakoiva huolto karsii keskiarvoa nopeammin rikkoutuvien laitteiden rikkoutumisen ja keskiarvoa pidempää kestävien laitteiden tarpeettoman huollon. (Collin & Saarelainen 2016, 75.)

Kun älykäs tuote on koko ajan verkon kautta etävalvonnassa ja -hallinnassa, voidaan etähuolto suorittaa hyvissä tapauksissa pelkällä ohjelmiston etäpäivityksellä. Sensorit tarvitsevat myös aika ajoin uudelleen kalibrointia, mutta tämäkin toimenpide voidaan huoltaa etänä tai asiakasta voidaan neuvoa etänä tekemään toimenpiteitä, jotka vaikuttavat tuotteen käyttöikään. (Collin & Saarelainen 2016, 76.)

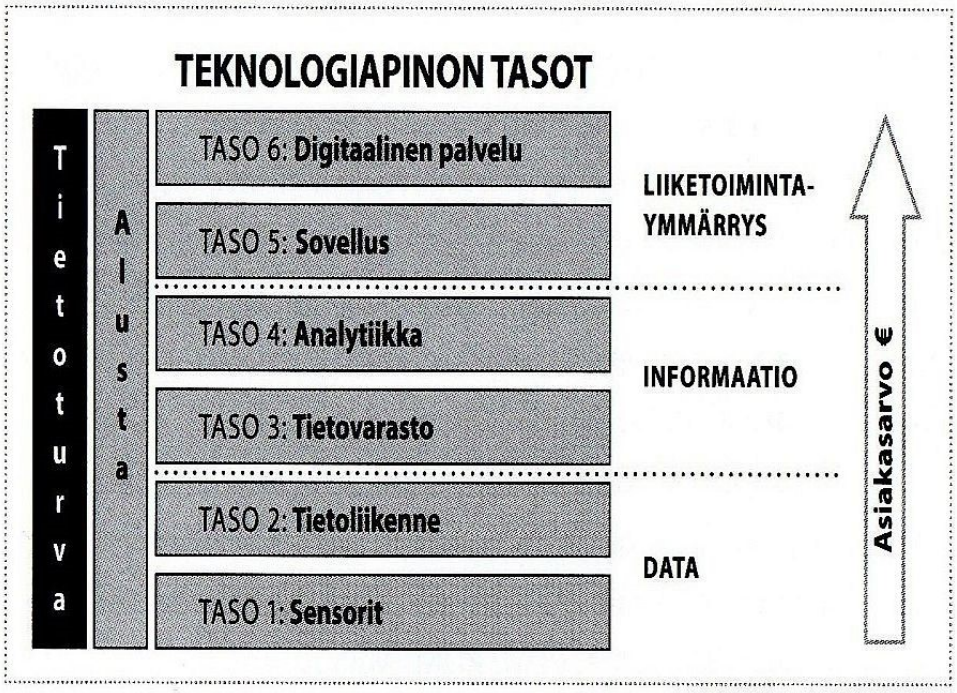
4 IOT TEKNOLOGIA

4.1 Infrastruktuuri

Älykäs verkko vaatii uudenlaisen ja monikerroksisen teknologiapinon suunnittelua ja rakentamista. Teollisen internetin infrastruktuuri pitää sisällään ohjelmistoja, sovelluksia, verkostoja, laitteistoa, tuotepilven, alustoja ja toimintaa säätteleviä sääntöjä (Ailisto ym. 2015, 13).

Älykkään verkon rakentamiseen teollista internetiä varten on jo teknologia olemassa. Ongelmaksi kuitenkin muodostuu, että kyse on teknologian eri osista. Älykkään verkon rakentamiseen ei ole valmista pakettia saatavilla, mikä sopisi kaikkiin tarpeisiin. Teknologian eri osia täytyy soveltaa, ja rakentaa omiin tarpeisiin sopiva teknologinen infrastruktuuri. (Collin & Saarelainen 2016, 141.)

Infrastruktuuria teollisessa internetissä kuvataan usein teknologiapinolla. Kuvassa 1 esitellään Collinin kuusitasoisen versio teknologiapinon tasoista. (Collin & Saarelainen 2016, 142.)



Kuva 1. Teknologiapino alhaalta ylöspäin. (Collin & Saarelainen 2016, 142)

Alimmalla eli ensimmäisellä tasolla toimivat kalustoon, koneistoon ja laitteistoon asennetut sensorit. Sensorit tuottavat mittausdataa toisella tasolla toimivalle tietoliikenteelle. Tietoliikenne huolehtii datan siirrosta ylemmille tasoille, mutta myös alimmalle tasolle, kun sensoreita esimerkiksi etähallitaan tai etäpäivitetään. Kolmantena tasona on tietovarasto, joka vastaa datan tallentamisesta esimerkiksi pilvipilvitietokantaan. Tietovarastoon voidaan tuoda dataa myös muistakin tietolähteistä kuin sensoreilta. Tasolla neljä käsitellään tallennettua datamassaa analytiikan välineillä. Viides taso, sovellustaso, muokkaa datan tietokone- ja mobiilisovelluksilla ihmisen havainnoitavaan muotoon. Ylin kuudes taso on Digitaalinen palvelu, joka ei periaatteessa kuulu teknologiapinoon, vaan on sen kaiken päällä. Digitaalinen palvelu luo yritykselle lisäarvoa ja mahdollisuuksia uusiin liiketoimintamalleihin. Se yhdistää asiakkaat, toimittajat ja muut avainkumppanit uusiin liiketoimintaprosesseihin ja -malleihin. Teknologiapino tarvitsee lisäksi teolliseen internetiin tarkoitettua alustaa, jotta pino toimisi alimmalta tasolta ylimmälle saakka. Alusta huolehtii tasojen yhteen toimivuudesta ja mahdollistaa hallinnan. Kaikessa tässä on mukana myös tietoturva, jonka pitää kattaa myös kaikki tasot. (Collin & Saarelainen 2016, 143.)

4.2 **Sensorit**

Sensorit toimivat IoT-teknologiapinon alimmaisena kerroksena ruohonjuuritasolla. Tämä taso on hyvin merkittävä osa esineiden internetin kannalta, koska se luo uutta dataa jatkuvasti ylimmille kerroksille analysoitavaksi. (Collin & Saarelainen 2016, 151.) Sensoreita voisi verrata toiminnaltaan ihmisen aisteihin, kun ihminen havaitsee mitä ympäristössään tapahtuu ja esimerkiksi silmät välittävät tietoa havainnoista aivoille. Sensorit havaitsevat myös ilmiöitä asennetussa laitteessa ja laitteen ympäristössä ja välittävät tiedon keskusjärjestelmälle. Ihminen tuntee nälkää, kun vatsalaukku alkaa olla tyhjä ja autossa polttoaineen merkkivalo syttyy palaa, kun sen sensori havaitsee, että tankin polttoaine on lähestymässä loppua.

Tässä opinnäytetyössä sensorien käsite on pelkistetty tarkoittamaan laitteita, tuotteita tai koneita, joihin kytketyt sensorit keräävät dataa niiden tilasta tai ympäristöstä ja lähettävät sen ylempiä kerroksia varten.

Sensori on pieni elektroninen laite, joka muuntaa erilaisia ilmiöitä koneilla luettavaksi sähköiseksi informaatioksi. Sensorit määritetään mittaamaan haluttuja ilmiöitä, jotka voivat olla joko fysikaalisia tai kemiallisia. Sensorit havaitsevat analogisia signaaleja, jotka muutetaan digitaaliseen muotoon, esimerkiksi erillisen A/D-muuntimen (analog to digital converter) avulla. Sensorit voivat olla joko passiivisia, jolloin ne toimivat vain informaation vastaanottimina tai aktiivisia sensoreita, jotka ovat vuorovaikutuksessa ympäristöön esimerkiksi lähettämällä ja vastaanottamalla radiosignaaleja. (Collin & Saarelainen 2016, 152.)

IoT:n kannalta tärkeässä roolissa ovat MEMS-anturit (micro electro-mechanical systems), mikrosysteemit, jotka ovat todella pieniä ja kuluttavat hyvin vähän virtaa. MEMS-anturilaite rakentuu keskusyksiköstä, joka voi prosessoida dataa, mikroprosessorista ja mikrosensoreista, jotka vuorovaikuttavat ympäristöön. MEMS-komponentin koko vaihtelee 1-100 mikrometrin välillä ja MEMS-anturilaitteen koko vaihtelee 20-1000 mikrometrin välillä. Sensorit sijaitsevat kuitenkin yleensä osana laitetta, jossa on myös mikroprosessori, virtalähde ja verkkoyhteys. (Collin & Saarelainen 2016, 156.)

Sensoreita on ollut jo kauan teollisissa laitteissa ja ne ovat olleet hyvin räätälöityjä tiettyä tarkoitusta kohden. Sensorit ovat toimineet aikaisemmin suljetuissa paikallisissa ympäristöissä ja vaativat säännöllistä huoltoa mekaanisesti jokaista sensoria kohden. Tänä päivänä sensorien hinta on saatu niin alas, että niiden määrä on noussut hurjasti ja yksittäisten sensorien huolto ja kalibroiminen käsin olisi liki mahdotonta. Kuitenkin sensorit ovat nykyisin kuin pieniä tietokoneita, joita ylläpitäjä voi hallita ja päivittää etänä esimerkiksi pilvipalvelualustalla. Suuri määrä sensoreita tarkoittaa myös hyvin suurta määrää dataa keskusjärjestelmiin, mutta sensorien oman paikallisen muistin ja mikroprosessorien ansiosta dataa on mahdollista käsitellä jo lähempänä datan syntypaikkaa. Datan esikäsittely keventää tietoliikennettä ja säästää esimerkiksi tilanteissa, joissa mittatulokset pysyvät suurimman osan ajasta tasaisina ja halutaan kerätä talteen vain poikkeamadataa. (Collin ja Saarelainen 2016, 152.)

Mitä suureita sensoreilla mitataan?

- kiihtyvyys, nopeus, asento, muu liike (mm. kiihtyvyysanturi, gyroskooppi)
- lämpötila, ilmankosteus
- kaasun/nesteen paine/ pinnankorkeus/virtaus (mm. paineanturi, barometri)
- kemiallinen ominaisuus/koostumus (mm. spektometri)
- värähtely
- vastus, virrankulutus, muu elekroninen ominaisuus
- säteily: näkyvä valo, infrapuna- ja ultaviolettisäteily
- valoisuus, läheisyys
- biometria (sormenjälki, iiris)
- äänenvoimakkuus
- säädata, kuten tuulen nopeus.

Sensoreille on monta erilaista tapaa syöttää virtaa, mutta virransyötön menetelmään vaikuttaa suuresti sensoreiden käyttötarkoitus ja sijainti. Sensoreiden virrankulutus on yleensä hyvin pieni ja tässä tapauksessa virtalähteeksi on usein valittu paristot tai akku, joita täytyy vaihtaa muutamien vuosien välein. Paristot tai akku eivät kuitenkaan aina ole viisas vaihtoehto sensoreille. Tehokkaampia virransyöttömenetelmiä joudutaan käyttämään tilanteissa, joissa suuri määrä sensoreita sijaitsee hankalassa ja laajassa lokaatiossa ja asentajan paristojen vaihto käy liian työlääksi. Toinen tilanne syntyy, kun sensorin virrankulutus kasvaa kohtuuttomaksi paristoille tai akulle. Paljon energiaa vaativia tilanteita ovat jatkuvasti mittausdataa lähettävät sensorit, paikannusjärjestelmän tai langattoman verkon radiopiirin käyttö. (Collin & Saarelainen 2016, 161.)

Tehokkaampien virransyöttö tekniikoiden käyttömahdollisuudet riippuvat ympäristöstä. Ihanteellisin ja vakain tapa syöttää sensoreille virtaa on PoE-teknologia (Power over Ethernet), joka edellyttää sensorien liittämisen kiinteään ethernet-verkkoon. PoE-teknologia mahdollistaa virransyötön ethernet-kaapelilla. Ympäristö usein rajoittaa kaapelien käyttöä ja tällöin on valittava luovempia langattomia virransyöttö teknologioita, joita ovat ympäristöstä energiaa keräävät (energy harvesting) sensorit, Power over Wifi-tekniikka (Po-WiFi) tai Wi-Carge. Ympäristöstä energian keräävät sensorit käyttävät hyödyksi eri olosuhteita, jokin sensori voi tuottaa kaiken tarvitsemansa energian pienellä aurinkopaneelilla ja toinen käyttää hyödyksi lämpötilaeroja. Po-Wifi-teknologia mahdollistaa sensorien tuottaa energiaa WLAN-reitittimen lähettämistä WiFi-radiosignaaleista. Wi-Carge-teknologia käyttää langattomaan energian siirtämiseen infrapunalaseria, mutta tämä tekniikka vaatii aina suoran näköyhteyden lähettimen ja vastaanottimen välille. (Collin ja Saarelainen 2016, 161.)

4.3 **Tietoliikenne ja älykkäät sensoriverkot**

4.3.1 IPv4 &IPv6

Kuten perinteisessä internetissä, niin myös IoT-verkoissa jokainen kytketty laite tarvitsee uniikin IP-osoitteen. Internet protokollaa tarvitaan siirtämään jokaista datapakettia internetissä. Protokolla on myös vastuussa tiedon reitittämisestä verkkolaitteiden välillä.

IPv4 on yleisimmin käytetty protokolla. Kyseisen version IP-osoitteiden koko on 32 bittiä, joka tarkoittaa 2^{32} uniikkia osoitetta. Luku vastaa noin 4,3 miljardia eri osoitetta, mutta käytännössä teoreettista maksimimäärää on mahdotonta saavuttaa, koska mm. verkkojen luokittelu vähentää osoitteiden määrää. Protokollan kehitysvuosina tämän osoitteiden määrän ajateltiin riittävän hyvin kattaakseen kaikki maailman verkkolaitteet. Internetiin liitettyjen verkkolaitteiden määrä on kuitenkin kasvanut nykyaikana räjähdysmäisesti ja IoT:n yleistymisen myötä kasvu vain kiihtyy. Verkkolaitteita on siis liitetty jo enemmän internetiin kuin IPv4:llä on tarjota uniikkeja osoitteita. IPv4-protokollan käyttöä ollaan onnistuttu pitkittämään NAT-laajennuksen avulla. (Guinard & Trifa 2016, 112.)

NAT-tekniikka sallii lokaalissa verkossa useampien laitteiden käyttää samaa yksittäistä julkista IP-osoitetta. Useimmat reitittimet ja palomuurit käyttävät NAT-tekniikkaa, josta on tullut tämän päivän IoT-verkkojen kulmakivi. NAT-tekniikka on kuitenkin vain tilapäinen päivitys ja ratkaisu ongelmaan, joka on edessämme tulevaisuudessa, kun verkkolaitteiden määrä jatkaa kasvua. Lisäksi NAT-tekniikka lisää verkon rakenteen monimutkaisuutta ja konfiguraation määrää. (Guinard & Trifa. 2016. 112.)

IPv6-protokolla on suunniteltu ratkaisemaan ongelma, kun tarkoitetaan uniikkien IP-osoitteiden riittävyyttä. IPv6 tulee kattamaan IoT:n vaatiman määrän IP-osoitteita, koska tämä versio perustuu 128 bittiä pitkiin osoitteisiin, joka vastaa 2^{128} uniikkia IP-osoitetta. Osoiteavaruuden laajentaminen tarkoittaa, että voisimme teoriassa asettaa IPV6-osoitteen jokaiselle atomille maanpinnalle ja silti osoitteita riittäisi tarpeeksi yli 100:lle maapallolle. (Guinard & Trifa 2016, 112.)

IPv6-protokollan käyttöönotto tulee kuitenkin olemaan työläs projekti, koska lähes kaikki verkkolaitteet toimivat nykypäivänä IPv4-versiolla. Koko internetin päivittäminen IPv6-protokollaa varten tarkoittaisi lähes kaikkien verkkolaitteiden päivittämistä tukemaan tätä versiota internetissä. Käytännössä siis käyttöjärjestelmien, tietokoneiden, palomuurien, puhelimien ja reitittimien tulee tukea IPv6-protokollaa. (Guinard & Trifa 2016, 113.)

4.3.2 Verkkotopologioita

IoT-verkko voidaan toteuttaa eri verkkotopologioita käyttäen, mutta yleisimmin käytetyt ovat point-to-point, tähtitopologiat tai mesh-topologia. Verkkotopologian käyttö riippuu paljon verkossa käytettävistä tiedonsiirtotekniikoista. Kaikki tekniikat eivät tue kaikkia topologioita.

Tiedonsiirtotekniikoiden luokittelussa tärkeänä tekijänä on etäisyys kahden verkkolaitteen välillä. Eri tekniikat voidaan luokitella sen mukaan, kuinka kaukana tai lähellä verkkolaitteiden pitää olla toisistaan, tai käytetäänkö yhteyden muodostamisessa verkkokaapeleita vai langatonta tekniikkaa. Verkkolaitteiden etäisyyksien vaihtelun vuoksi syntyy haasteita IoT-verkon luomiseen, koska eri etäisyydet vaativat eri verkkotekniikoita. Pitkä etäisyys langattomassa verkossa vaatii viestin lähettämiseen enemmän tehoa, joka lisää virrankulutusta. Tekniikoiden välillä on myös eroja datapakettien välittämisessä, koska eri tekniikat käyttävät datapakettien lähettämisessä eri menetelmiä, jotka vaikuttavat tiedonsiirron ominaisuuksiin. (Guinard & Trifa 2016.)

Point-to-point verkkotopologia on yksinkertaisin tapa liittää verkkolaitteet toisiinsa. Topologiassa kaksi verkkolaitetta muodostavat suoran yhteyden toisiinsa kommunikaatiota varten. Point-to-point mallia käytetään hyväksi etenkin puettavassa tietotekniikassa. Esimerkiksi käyttäjä voi yhdistää bluetooth-parin älykkään sykemittarin ja älypuhelimen välille. Tiedonsiirtoa varten voi käyttää myös Wi-Fi ad hocia, joka soveltuu point-to-point topologiaan. (Guinard & Trifa 2016.)

Tähtitopologiassa on yksi keskuslaite, jonka kanssa kaikki muut verkkolaitteet kommunikoivat. Keskuslaitteena toimii yleensä kytkin tai keskitin. Keskuslaitteeseen kytketyt verkkolaitteet eivät välttämättä välitä toisistaan lainkaan. Keskuslaitteeseen voidaan kuitenkin kytkeä toinen keskuslaite, jolloin muodostuu useamman tähden verkko. Esineiden internetissä matkapuhelinverkot toimivat usein tähtitopologialla, kun matkapuhelimet muodostavat yhteyden lähimpään tukiasemaan. Tähtitopologia voi olla käytössä esimerkiksi kodin automaatiojärjestelmässä, jossa kodin älylamput kommunikoivat eri yhdyskäytävien kautta keskuslaitteelle. Tiedonsiirtotekniikkana voi toimia tässä tapauksessa esimerkiksi ZigBee tai reititin Ethernetillä. (Guinard & Trifa 2016.)

Mesh-topologiassa ei ole keskuslaitetta, koska kaikki verkkolaitteet pystyvät välittämään viestin oikeaan paikkaan viereisen laitteen kautta. Kaikki verkkolaitteet ovat siis suorassa yhteydessä toisiinsa ja viestin reitin voi määrittää tehokkaammaksi hopsien ja relaysien avulla. Viesti kulkee verkossa samalla periaatteella kuin reitittimet etsivät oikeat IP-osoitteet internetissä. Verkkoa voidaan laajentaa lisäämällä uusia verkkolaitteita tai verkosta voi tehdä vakaamman, jolloin viestiketju ei katkea, vaikka yksi verkkolaite ketjusta hajoaisikin. Muut verkkolaitteet havaitsevat rikkoutuneen verkkolaitteen ja kääntävät reitin varareitille. (Guinard & Trifa 2016.)

IoT:ssa mesh-topologia on hyödyksi varsinkin syrjäisillä seuduilla, joissa on huono kuuluvuus mobiilidataa varten. Syrjäisessä metsässä voidaan tarkkailla esimerkiksi saasteiden määrää kytkemällä mittauslaitteet kommunikoimaan mesh-verkossa. Syrjäisen metsän verkkoa on mahdollista monitoroida etänä, jos mesh-verkossa on vähintään

yksi verkkolaite, johon saadaan riittävä 3G/4G/5G tai satelliittiyhteys. Mesh-topologiaa tukevat ainakin IoT:n verkkotekniikoista ZigBee ja 6LoWPAN. (Guinard & Trifa 2016.)

Verkkotopologiat voidaan jakaa kahteen ryhmää riippuen verkon laitteiden välisestä etäisyydestä. Lyhyttä etäisyyttä kuvaa PAN (Personal Area Network) ja pitkää etäisyyttä kuvaa WAN (Wide Area Network).

4.3.3 PAN-tiedonsiirtotekniikat

Personal Area Networking (PAN) tiedonsiirtotekniikat ovat käytössä IoT-verkoissa, joissa verkkolaitteiden tai älykkäiden esineiden etäisyydet toisistaan ovat pienet. Tämä protokolla on laajassa käytössä IoT-sovelluksissa ja järjestelmissä, koska se tarjoaa houkuttelevan kompromissin viestintäpeiton ja virrankulutuksen välillä. Sopivia järjestelmiä ovat esimerkiksi älyvaatteet, älytermostaatti tai autotallin oven kauko-ohjaus järjestelmä. PAN-tekniikoita on olemassa hyvin monta, joten esittelen vain yleisimpien käytössä olevien tekniikoiden ominaisuuksia. (Guinard & Trifa 2016.)

IEEE 802.15.4 standardi on kehitetty langattomaksi tiedonsiirtotekniikaksi pienitehoisille, edullisille ja alhaisten datanopeuksien verkkolaitteille kommunikointia varten lyhyille etäisyyksille. Nämä ominaisuudet sopivat erinomaisesti IoT-verkkoihin sisätiloihin kodin automaatiojärjestelmiin, joissa on rajalliset resurssit. Standardi soveltuu myös teolliseen käyttöön, kuten esimerkiksi rakennusautomaatioon, teolliseen valvontaan ja sovellusten kontrollointiin. Tätä standardia käytetään usein perustana monissa IoT PAN verkkotekniikoissa. (Guinard & Trifa 2016.)

Yhtenä suurena haittapuolena IEEE 802.15.4 tekniikassa on, että se ei pysty kommunikoimaan suoraan toisten laitteiden kanssa internetin läpi TCP/IP:llä tai UDP:llä. Tämä rajoitus on johtanut uuden tiedonsiirtotekniikan 6LoWPAN (IPv6 over low-power wireless personal area networks) kehittämiseen, joka sallii eri verkoissa olevien 6LoWPAN-laitteiden kommunikoinnin keskenään. Tekniikka mahdollistaa IPv6 pakettien lähettämisen ja vastaanottamisen IEEE 802.15.4 tekniikkaan perustuvien verkkojen läpi. 6LoWPAN on kehitetty nimenomaan IoT:ta varten mahdollisimman pieniin ja tehoiltaan rajattuihin tuotteisiin kuin mahdollista. IPv6-protokolla sopii paremmin IoT:lle laajemman osoiteavaruuden takia. Ongelmana on kuitenkin eri valmistajien käyttämät eri protokollapinot, jotka eivät ole yhteensopivia. (Guinard & Trifa 2016.)

ZigBee on yksi yleisimmin käytetyistä IEEE 802.15.4 standardiin perustuva matalan virrankulutuksen WPAN-verkkoteknologia, jonka kehittäjä on kattojärjestö ZigBee Alliance. Zigbeetä käytetään laajasti sulautetuissa järjestelmissä teollisuudessa, terveydenhoidossa ja kodin automaatiossa. ZigBeen erityisominaisuus on dynaaminen meshverkkojen tuki, mutta sitä voi käyttää myös tähti- tai puutopologiassa. ZigBee skaalautuu paljon laajemmaksi kuin vain fyysisen tason tiedonsiirtotekniikaksi, aina sovellustasolle asti. (Guinard & Trifa 2016.)

ZigBee-radiopiirit ovat erittäin halpoja ja omaavat hyvin pienen virrankulutuksen, koska niillä on ominaisuus pysyä lepotilassa pitkiäkin aikoja. ZigBeen tiedonsiirtonopeus on pieni verrattuna muihin 802.15.4 teknologioihin, mikä on hyvä virrankulutuksen kannalta, mutta tiedonsiirto on hitaampaa. Zigbeen selviä haittapuolia ovat heikko

yhteensopivuus muihin protokolliin, haavoittuva tietoturva ja epävakaat yhteydet. ZigBee käyttää samoja avoimia taajuuksia kuin WLAN ja Bluetooth, jotka ovat ruuhkaisia ja aiheuttavat yhteysongelmia. (Collin & Saarelainen 2016, 175.)

Bluetooth on hyvin suosittu langaton tiedonsiirtotekniikka lyhyille etäisyyksille. Bluetoothia tukevat lähes kaikki mobiililaitteet ja hyvin monissa tapauksissa IoT-verkkolaitteet käyttävät älypuhelinta yhdyskäytävänä internetiin, esimerkiksi älyvaatteissa. IoT-verkkoja varten on kehitelty oma versio Bluetooth Low Energy (BLE), joka kuluttaa vähemmän virtaa ja soveltuu hyvin paristollisille laitteille. BLE:n suosiota lisää myös sen edullinen hinta, soveltuvuus mobiililaitteiden tekniikan kanssa ja sovelluskehityksen helppous. Lisäksi Bluetooth voi käyttää tietoliikenteessä 128-bittistä AES-salausta. Bluetoothin kantama on lyhyt, tyypillisesti alle 50m, joka soveltuu hyvin yksinkertaisiin yhteyksiin. (Guinard & Trifa 2016.)

Kuluttajien käytössä yleisesti bluetooth-laitteet muodostavat yhteyden (bluetooth-pari), jossa yhdistynyt laite on joko isäntä (master), tai alainen (slave). Esimerkiksi älypuhelin yhdistetään bluetoothilla langattomiin stereoihin. Kuitenkin teollisessa käytössä verkkomallit monimutkaistuvat ja bluetooth-laitteita tulee lisää samaa verkkoon. Bluetoothin rajoitteita ovat olleet lyhyt kantama ja verkkomalli, joka kuuluu hub-and-spoke-periaatteeseen, jossa päätelaitteiden tietoliikenne keskitetään yhteen pisteeseen.

Bluetoothin rajoitteet teollista internetiä varten ovat olleet huomattava etu kilpaileville lyhyen kantaman tekniikoille, joissa 802.15.4 standardit mahdollistavat mesh-topologian käytön. Täten Bluetooth SIG järjestö julkaisi mesh-määritykset kesällä 2017, joten Bluetooth 4.0 tai uudempia versioita tukevat laitteet voidaan päivittää tukemaan mesh-verkkoja. Bluetoothiin perustuvat verkot pystyvät nyt siis laajentumaan huomattavasti suuremmalle alueelle, koska yksittäinen bluetooth-päätelaite tarvitsee nyt vain yhden päätelaitteen kantamalleen kommunikoidakseen koko verkon kanssa. (Collin & Saarelainen 2016, 175.)

Thread on yksi uusimmista IoT-tiedonsiirtotekniikoista ja käyttötarkoitus on suunniteltu laitteiden liittämistä ja kontrollointia varten kotona. Teknologia perustuu IEEE 802.15.4 standardiin, ja se tukee mesh-topologiaa. Erona muihin teknologioihin on, että Thread uudelleen käyttää avoimia standardeja, kun mahdollista, ja toteuttaa verkkokerroksen 6LoWPAN:lla, jotta se voi kommunikoida laitteiden kanssa suoraan internetissä. Thread käyttää kuljetuskerroksessa UDP:ta, mutta se ei kata täsmällisesti sovelluskerrosta. Thread vaatii lisättävän tietokoneohjelman ja se tukee vaihtelevasti internet sovelluskerroksen eri standardeja, mikä eroaa ZigBeestä ja Bluetoothista. (Guinard & Trifa 2016.)

Thread sallii suurien mesh-verkkojen toteutuksen, joissa 250-300 laitetta voidaan kytkeä verkkoon talossa tai rakennuksessa. Tämän tekniikan hyviä ominaisuuksia on pieni latenssi (<100ms) ja energiatehokkuus, joka sallii pattereilla toimivien laitteiden käydä useita vuosia. (Guinard & Trifa 2016.)

Wi-Fi (Wireless fidelity) on IEEE 802.11 WLAN standardiin perustuva langaton tiedonsiirtotekniikka koteihin ja yrityksille. Wi-Fi on hyvin yleisesti käytössä, koska se on nopea tiedonsiirrossa verrattuna muihin langattomiin verkkoihin ja isona etuna on sen soveltuminen suoraan ethernet-verkon topologiaan ja standardeihin. Wi-Fiä tukevat arkiset elektroniikkalaitteet yleistyvät jatkuvasti kuluttajien keskuudessa, kuten esimerkiksi TV, mikroaaltouuni, musiikintoistolaitteet ja monet muut. (Guinard & Trifa 2016.)

Kuitenkin useimmat Wi-Fi-tekniikat (802.11a-n) ovat rajoittuneita joillekin IoT sovelluksille. Suurimpana haittana on, että Wi-Fi kuluttaa paljon virtaa, joka lyhentää paristollisten laitteiden käyttöä huomattavasti. Toisena suurena huolena on Wi-Fi-tukiasemien signaalin kuuluvuus, jossa kaikkien WLAN:iin kytkettyjen laitteiden täytyy olla tukiaseman peiton sisällä ja signaalia rajoittaa helposti eri esteet, kuten esimerkiksi betoniseinät. (Guinard & Trifa 2016.)

Näihin ongelmiin ollaan kuitenkin kehitetty ratkaisuksi Wi-Fi HaLow, standardi IEEE 802.11ah, joka on optimoitu IoT:ta varten. Uudessa standardissa ollaan kehitetty nimenomaan IoT:n vaatimia ominaisuuksia ja sen hyviä puolia ovat rakenteiden läpäisykyky, jopa kilometrin kantama, vähäinen virrankulutus ja laitteiden suuri lukumäärä liitettynä samaan verkkoon. (Guinard & Trifa 2016.)

EnOcean on hieman tuntemattomampi langaton teknologia, jota käytetään pääsääntöisesti rakennuksissa ja muissa teollisuusratkaisuissa. Tämä teknologia on kehitetty ratkaisemaan ongelma energiankulutukseen, ja se salliikin verkkolaitteiden kerätä virtaa ympäristöstä erilaisilla ratkaisuilla, joita ovat esimerkiksi sähkömagnetismi, kineettinen energia, aurinkovoima, lämpösähkömuuntajat. EnOcean määrittely kattaa fyysisen ja verkkokerroksen, mutta se tarjoaa myös lisämäärittelyjä sovelluskerrokselle. EnOcean tekniikka on patentoitu oma standardi ISO/IEC 14543-3-10, joten tekniikka vaatii käyttöön EnOceanin omat langattomat lähetin-vastaanotinmoduulit yhdyskäytävää varten, jotta se voi vastaanottaa viestejä EnOcean verkkolaitteilta. Teknologian energiankulutus on hyvin pieni ja se säästää aikaa ja materiaaleja, koska verkkolaitteet ovat langattomia ja patterittomia. (Guinard & Trifa 2016.)

PAN-tiedonsiirtotekniikat ovat tarkoitettu toimimaan lyhyillä etäisyyksillä, ja suurimmaksi osaksi sisätiloissa. Ympäristö luo omat haasteensa verkkolaitteiden langattoman signaalin lähetykseen tekniikasta riippumatta, koska sisätiloissa signaalin vahvuuteen vaikuttavat paksut seinät ja muut häiriöt. Tukiasemiin perustuvien tekniikoiden kantamat rajoittuvat ominaisuuksiin luoda yhteydelle peittoalue, kun taas mesh-topologiaa tukevat tekniikat voivat periaatteessa lisätä kantamaa lisäämällä verkkolaitteita. Verkkolaitteiden määrä kuitenkin lisää verkon monimutkaisuutta. (Guinard & Trifa 2016.)

Lyhyillä etäisyyksillä on erittäin suurella todennäköisyydellä mahdollista käyttää rakennuksien verkkolaitteiden virtalähteenä virtapistoketta. Energiankulutus ei tällöin ole haasteena ja oiva vaihtoehto langattomaan tiedonsiirtoon on Wi-Fi. Paras vaihtoehto ympäristön salliessa on kuitenkin Ethernet, koska langallinen tiedonsiirto on aina vakaampaa kuin langaton. PoE:n käyttö sallii myös virran siirron verkkokaapelin kautta esimerkiksi kiinteässä sijainnissa olevalle WLAN-tukiasemalle, mikä on ihanteellinen tapa luoda verkko käyttäen sekä Ethernetiä, että WiFiä. (Guinard & Trifa 2016.)

4.3.4 WAN-tiedonsiirtotekniikat

Wide Area Networks -tekniikat soveltuvat verkkoihin, joissa haasteina on verkkoon kytkettävien laitteiden suuri lukumäärä tai maaston luomat pitkät etäisyydet. WAN verkoissa voi olla kytkettynä satoja tai tuhansia verkkolaitteita, ne voivat sijaita hyvinkin laajalla alueella, kuten esimerkiksi metsässä tai kaupungissa. Periaatteessa olisi myös mahdollista toteuttaa laajalla alueella IoT-verkon kaikkien verkkolaitteiden monitorointi käyttämällä hyväksi PAN-tekniikoista esimerkiksi ZigBeetä, koska se tukee meshtopologiaa. Todella laajoista mesh-verkoista tulee kuitenkin erittäin monimutkaisia ja kalliita, koska ne vaativat lisää yhdyskäytävien, toistimien ja vahvistimien lisäämistä verkkoon. Lisälaitteet kuluttaisivat myös enemmän pattereita. IoT:ta varten on kehitetty paljon erilaisia WAN-tekniikoita, mutta yleensä niillä on yhteisenä piirteenä tähtitopologia, jossa on vähäenergisiä verkkolaitteita, jotka kommunikoivat suoraan tehokkaan yhdyskäytävän, kuten antennin tai tukiaseman kanssa. Hyvä esimerkki WAN:sta on mobiiliverkko. (Guinard & Trifa 2016.)

Kaikista yleisin tapa liittää älykkäät esineet IP-verkkoon langattomasti, on käyttää mobiiliverkkojen internetyhteyttä, joka voi olla GPRS, 3G, 4G, tai miksei myös SMS. On olemassa useita sulautettuja järjestelmiä, jotka tukevat mobiilidataa joko natiivisti tai asennetuilla lisäosilla. (Guinard & Trifa 2016.)

Kuitenkin haittapuolena puhelinliittymien käytössä on, että niitä ei ole suunniteltu IoT:ta varten. Mobiilidatan käyttö kuluttaa paljon virtaa, minkä on varmastikin jokainen älypuhelimen omistaja huomannut. Esimerkiksi suomalainen Espotelin Enevo käyttää 3G-verkkopiiriä järjestelmässään, jossa tarkkaillaan jäteastioiden täyttöastetta. Järjestelmä kuluttaa tietysti enemmän virtaa, mutta iso paristo vaatii myös suuremman kotelon. Molemmat tekijät nostavat palvelun kokonaisuuden hintaa. (Collin & Saarelainen 2016, 171.) Mobiilidatan jatkuva käyttö kommunikointiin ei siis ole hyvä vaihtoehto paristollisille laitteille. Toinen rajoite mobiiliverkoissa on, että niitä ei ole tarkoitettu miljardeille esineille. Tukiasemat pystyvät käsittelemään rajoitetun määrän esineiden pyyntöjä tietyssä ajassa, joten antenneja täytyisi asentaa lisää ja paljon. Lopuksi, mobiiliverkkojen käyttö on suhteellisen kallista, koska hinnoittelu on luotu yhtä liittymää varten ja tämä ei mukaudu IoT:n tarpeisiin. Nykyiset mobiiliverkot ovat siis todella rajoittuneita ja ehdollisia ratkaisuita IoT:ta varten. (Guinard & Trifa 2016.)

Mobiiliverkkojen ongelmiin ollaan pureuduttu ja 4G-standardeja kehitetään jatkuvasti. 4G/LTE (Long Term Evoluation) odotetaan olevan vahva vaihtoehto langattomaan verkottamiseen, koska IoT:n tarpeisiin kehitetyt uudet standardit kuluttavat vähemmän virtaa. Uusia standardeja ovat LTE-M, NarrowBand IoT (NB-IoT) ja NarrowBand LTE (NB-LTE). Standardien sarjapiirit eroavat toisistaan painottamalla tiettyä ominaisuutta. LTE-M on suoraa yhteensopiva 4G/LTE -verkon kanssa, NB-IoT on erityisen virtapihi ja NB-LTE, jonka takana on myös Nokia, on merkittävän halpa. 4G-standardeja voidaan pitää IoT:n kannalta esimakuna tulevalle 5G mobiiliverkolle. (Collin & Saarelainen 2016, 171.)

Tulevina vuosina miljardit esineet ovat liittymässä internetiin ja tätä varten NGMN (Next Generation Mobile Networks) Alliance on kehittämässä uutta 5G mobiiliverkkoa. Yhdistykseen ja kehitystyöhön kuuluvat maailman suuret matkapuhelinoperaattorit, tavarantoimittajat, valmistajat ja tutkimuslaitokset, mutta Suomessa suurin kehittäjä on Nokia, joka aloitti vuonna 2017 5G-verkon rakentamisen, vaikka käytettäviä 5G-tekniikan standardeja ei ole vielä päätetty. (Guinard & Trifa 2016.)

IoT:ta varten erityisesti suunnatun 5G-verkon odotetaan tulevan kaupalliseen käyttöön 2020-luvulla ja sen tarkoitus on tuoda mukanaan useita parannuksia mobiiliverkkoihin. Se tulee olemaan paljon energiatehokkaampi ja antennit tai yhdyskäytävät tulevat sallimaan huomattavasti useamman laitteen pyynnön samanaikaisesti. 5G:ssä tavoitellaan saavutettavaksi jopa satakertainen kyky välittää tietoliikennettä ja vähintään kymmenen vuoden akkukesto. Lisäksi se suunnitellaan tukemaan mesh-topologiaa, joka tulee parantamaan mobiiliverkon kenttää ja energian käyttöä. Teollisen internetin näkökulmasta houkuttelevia parannuksia tulee ensinnäkin 5G liittymien hinnoitteluun, joka muutetaan vastaamaan paremmin IoT:n tarpeisiin. Toiseksi 5G:llä pyritään saavuttamaan hyvin pieni yhden millisekunnin latenssi, josta tulee todella tärkeä tekijä latenssikriittisissä ympäristöissä, kuten esimerkiksi robottien etäohjauksessa. (Collin & Saarelainen 2016, 171.)

Nykyinen mobiiliverkko on soveltunut huonosti IoT-sovelluksia varten, mikä on synnyttänyt lukuisia erilaisia IoT:lle perustuvia tekniikoita, jotka kulkevat termin low-power wide area networks (LPWAN) alla. Käytännössä nämä uudet tekniikat tarjoavat hyvin samaa asiaa eri tekniikalla, mutta suurimmalle osasta tekniikoista tyypillinen piirre on tähtitopologia; useat vähävirtaiset verkkolaitteet kommunikoivat suoraan voimakkaiden tukiasemien kanssa, jotka ovat suoraan yhdistetty sähkö- ja ip-verkkoon. Tästä arkkitehtuurista on myös syntynyt yksi LPWAN:n suurin haaste, joka on oman verkkoinfrastruktuurin asentaminen. Nämä erikoisverkot vaativat asentamaan ylimääräisiä antenneja maastoon samalla periaatteella kuin mobiiliverkon operaattori asentaa omia mastoja. (Guinard & Trifa 2016.)

Markkinoiden johtava LPWAN tekniikka on SigFox, joka oli myös ensimmäinen laajalle levittäytynyt IoT:lle omistettu LPWAN operaattori. SigFoxilla on laaja kenttä monissa Euroopan maissa, kuten myös Suomessakin. Kilpailu alalla on kuitenkin tiukkaa ja muita kilpailevia suuria verkkoja ovat LoRa, nwave ja Weightless Alliance. Suomessa sertifioitiin ensimmäisenä maailmassa LoRa-testauspalveluita tarjoava yritys suomalaisen Espotelin toimesta vuoden 2015 lopulla. (Collin & Saarelainen 2016, 171.)

LPWAN:lla on monia hyötyjä. Ensinnäkin, verkkoinfrastruktuurin asentaminen on operaattorin vastuulla, mikä tekee verkoista loppukäyttäjälle käyttöystävällisen. Toiseksi, tukiasemien yhteyden kantama riittää melko pitkälle, joka on useita kilometrejä riippuen käytettävästä tekniikasta. Lisäksi jokainen tukiasema kykenee käsittelemään huomattavan määrän päällekkäistä liikennettä. Potentiaalia löytyy jopa miljoonien älykkäiden esineiden yhdistämiseen yhteen tukiasemaan. Lopuksi, energiankäyttö on paljon matalampi verrattuna verkkoihin, jotka käyttävät WAN tai PAN protokollia. LPWAN:lla voi pidentää esimerkiksi AA paristojen (noin 2,5 Ah) käyttöä jopa 20 vuoteen. (Guinard & Trifa 2016.)

LPWAN on keskittynyt enimmäkseen teollisuutta varten ja suoraan kaupan hyllyltä ostettujen laitteiden liittäminen verkkoon on monimutkaisempaa kuin PAN verkkoon. LPWAN verkot ovat usein myös yksityisomisteisia ja suljettuja ekosysteemeitä, joten verkkoon liitetyt laitteet soveltuvat ja lukittuvat vain ja ainoastaan kyseiseen verkkoon. Toisaalta on saatavilla esimerkiksi LoRa- ja Sigfox-tuen omaavia yhdistelmämodeemeja. LPWAN on siis täydellinen tilanteissa, joissa on matala kaistanleveys ja kerätään dataa älykkäästä mittarista, mutta todella kankea käyttää esimerkiksi autotallin oven avaukseen. Tekniikka on haasteellinen ja erittäin hidas käskyjen lähettämiseen laitteille, koska esimerkiksi Sigfoxilla on 12 tavun viestin maksimikoko ja päivittäinen 140 viestin maksimimäärä. (Collin & Saarelainen 2016, 171.)

4.3.5 Muut langattomat tekniikat

Near-field communications on lähiluentaan tarkoitettu langaton radioteknologia, jolla on rajoittuneet käyttömahdollisuudet. Signaalin kantama on todella lyhyt, joka on turvallisuussyistä rajattu noin seitsemään senttimetriin. Tekniikan käytössä suuri etu on, että melkein kaikista älypuhelimista löytyy NFC ominaisuus ja tätä hyödynnetäänkin lähinnä mobiilimaksamisessa ja mobiilipuissa. (Collin & Saarelainen 2016, 171.)

Radio frequency identification on ollut jo kauan iso osa logistiikan toiminnassa. Rfid perustuu esineiden tunnistamiseen radiotaajuuden avulla. Esineille luodaan identiteetti, joka on periaatteeltaan sama kuin intenetin ip-osoite. Rfid:n avulla saadaan yksilöityä esineet tietojärjestelmiin suurissakin logistiikka ympäristöissä. (Collin & Saarelainen 2016, 171.)

Esineisiin tai tuotteisiin kiinnitetään rfid-tunniste, jota nimitetään myös rfid-tagiksi. Tageja luetaan rfid-lukijalaitteilla ja -antennijärjestelmillä, jotka välittävät tiedon esineistä taustajärjelmälle. Rfid-tagit ovat hyvin pieniä ja halpoja kiinnitettäviä osia, jotka voidaan jakaa aktiivisiin ja passiivisiin tageihin. Aktiivisilla tunnisteilla voidaan sekä lähettää, että vastaanottaa radiokyselyitä, kun passiiviset rajoittuvat pelkästään tiedon lähettämiseen. Rfid-radion kantama on aktiivisella tunnistimella muutamia kymmeniä metrejä ja passiivisella tunnisteella kantama jää enintään muutamaan metriin. Aktiivisissa tageissa on pieni paristo, mutta passiiviset tagit keräävät virtansa läheisen lukijalaitteen radioaalloista. (Collin & Saarelainen 2016, 171.)

Rfid-teknologialla pystyy korvaamaan viivakoodien skannauksen ja teknologiaa käytetään esimerkiksi tuotantolaitoksissa seuraamaan sijaintia yksittäisistä tuotteista, joita on hyvin suuri määrä. Tuotteiden tarvitsee kulkea luentapisteiden kautta, jotta niitä voidaan seurata. Tuotteista saadaan samalla luettua rfid-tagin tiedot automaattisesti ja ne voidaan päivittää suoraan tietojärjestelmään. (Collin & Saarelainen 2016, 171.)

4.4 **Protokollat ja standardit**

Protokollat ja standardit ovat tärkeitä apuvälineitä tiedonsiirrossa, kun data liikkuu sensoreilta tietokantaan ja koneilta koneille. Nämä apuvälineet mahdollistavat datan virtaamisen sujuvasti verkotetussa arvoketjussa koneiden, järjestelmien ja ohjelmistojen välillä. Standardien avulla järjestelmiin voi kytkeä uusia laitteita nopeasti ”plug-and-play-tekniikoilla”. Kuitenkin standardit saattavat myös rajoittaa laitteiden ja järjestelmien yhteensopivuutta, jos ne ovat suljettuja, tietyn valmistajaryhmän tunnustamia, yhden valmistajan tai ainoastaan kansallisia. Tällöin käyttäjä jää niin kutsuttuun toimittajaloukkuun, joka voi olla hyvin ongelmallinen, koska kilpailevia standardeja on kehitetty monia ja heikommat standardit putoavat kehittyneempien standardien tieltä. (Collin & Saarelainen 2016, 181.)

Protokollat eroavat ominaisuuksiltaan niiden käyttötarkoituksen, kehitystilanteen, tietoturvan ja suorituskyvyn mukaan. Käyttötarkoituksesta riippuen protokollan ominaisuudet voivat erota toisistaan huomattavasti korostaen joko tietoliikenteen viestinnän nopeutta ja keveyttä tai äärimmäistä luotettavuutta. Esimerkiksi älykkään palovaroitinjärjestelmän etähallinta tarvitsee luotettavaa tietoliikennettä. Palohälyttimille pitää olla jatkuva yhteys keskusjärjestelmään ja tietoliikenteessä ei saa ilmetä datapakettien hävimistä. (Collin & Saarelainen 2016, 181.)

Protokollat voidaan jakaa tiedonsiirron periaatteiden mukaisesti kahteen ryhmään. Ensimmäinen on julkaisija-tilaaja-malli ja toinen on asiakas-palvelin-malli. Julkaisija-tilaaja-mallissa dataa tuottavat lähdejärjestelmien päätelaitteet ovat julkaisijan roolissa ja lähettävät dataa eteen päin kohti datan tilaajaa. Määritellystä aiheesta julkaistu data kulkee automaattisesti tietoverkossa yleensä keskitetylle pisteelle, joka edelleen välittää datan kohteeseen, joka on tilaajan roolissa. Tilaajana voi toimia keskitetty tietokanta, eri sovellukset tai toinen päätelaite. Päätelaite voi käyttää molempia rooleja oman toiminnan avuksi, se voi siis olla samaan aikaan tilaajan ja julkaisijan asemassa. Asiakas-palvelin-mallissa tiedonsiirto tapahtuu aina kun asiakas kyselee sitä palvelimelta. Tällä on pieni verkon kuormitus, koska dataa lähetetään vain sitä pyydettäessä. Teollisessa internetissä palvelimen rooli voi olla sensoroidulla päätelaitteella, jonka tarkoitus on välittää kerättyä dataa asiakkaana toimivalle järjestelmälle. Data virtaa pelkästään kyselyn aikana, joten päätelaitteilla on oltava oma paikallinen puskuri, josta suodatettu ja pakattu data säilyy pyyntöön asti. Haittapuolena mallissa on, että langattomien verkkojen täytyy jatkuvasti tehdä kyselyjä päätelaitteille, että ne ovat hereillä ja valmiina lähettämään dataa pyydettäessä. Kyselyt kuluttavat akkua ja ovat oikeastaan turhaa tietoliikennettä. (Collin & Saarelainen 2016, 181.)

Protokollia täytyy kehittää usein vanhojen ja uusien laitteiden väliin teolliseen internetiin siirryttäessä, koska tehtaan jo käyttämät tuotantovälineet on tarkoitettu pieneen automaatiojärjestelmään. Tuotantokaluston uudistaminen kokonaan on hyvin kallis investointi, joten edullisempi ratkaisu laitteiden liittämiseksi internetiin on usein protokollamuuntimien käyttö. Protokollamuuntimissa piilee kuitenkin aina riski, että datan eheys kärsii tai data voi muuttua kokonaan epäluotettavaksi. Lisäksi yritykselle voi muodostua useita eri järjestelmien saarekkeita standardiongelmien takia. (Collin & Saarelainen 2016, 181.)

Standardoinnin puutteet, fragmentoituminen ja suljetut valmistajien ratkaisut ovat vielä toistaiseksi ongelmana teollisessa internetissä. Ongelmaan ollaan kuitenkin herätty ja sitä koittavat ratkaista monet suuret eri yrityksien liittoumat, joissa voi olla satojakin jäseniä. Kuitenkin nämä liittoumien väliset kilpailut IoT-standardien kehittämisestä muodostavat itsessään jo ongelman, koska siitä voi seurata päällekkäisiä standardeja, jotka yrittävät ratkaista samoja ongelmia. (Collin & Saarelainen 2016, 181.)

Yksi suurimmista esineiden internetin standardointihankkeista on IEEE P2413, jossa on mukana noin 200 maailman johtavaa yritystä monelta toimialalta ja teknologian yritystä. Standardointihankeen tavoitteena on luoda arkkitehtuurikehys, joka mahdollistaisi järjestelmien yhteensopivuuden ja datan jakamisen IoT-järjestelmissä teollisuudessa, liikenteessä, kotiautomaatiossa ja muilla sovellusaloilla. (Collin & Saarelainen 2016, 181.)

4.5 **Tietovarasto**

Teollisen internetin yksi tarkoituksista on kerätä enemmän raakadataa sensoreilla tietovarastoihin, jotta analytiikan avulla raakadatasta saadaan jalostettua hyödynnettävää tietoa. Sensoreiden keräämän datan määrä voi olla mielettömän suuri ja datan laatu voi vaihdella sisältäen myös kuvia tai videoita. Sensoreiden määrän kasvaessa jopa tuhansiin kappaleisiin, voi kerääntyä hyvin paljon dataa keskitettyyn tietovarastoon, jolloin on hyvin tärkeää, ettei datan varastoinnista synny pullonkaulaa. Tietovaraston on skaalauduttava sujuvasti ja vastaanotettava datamassoja hyvin nopeasti virheittä. Suuria datamassoja voidaan tiivistää algoritmeilla ja esikäsittelemällä dataa sensoreissa, mutta toisaalta levytilan hinta laskee jatkuvasti. (Collin & Saarelainen 2016, 195.)

Tietovarasto on mahdollista luoda rakenteeltaan hyvin monilla eri tyypeillä ja datan prosessointi riippuu tietokannan tyypistä. Teollisen internetin toiminnan vaatimuksista riippuen dataa täytyy käsitellä todella nopeasti, välillä jopa lähes samanaikaisesti kun se syntyy tai hitaammin analysoimalla data jälkikäteen. Tietovaraston rakenteen tyypit voidaan jakaa raa'asti SQL ja NoSQL -tietokantoihin tai keskitettyyn ja hajautettuun arkkitehtuuriin. (Collin & Saarelainen 2016, 196.)

4.5.1 SQL- & NoSQL-tietokannat

Maailman suosituimmat tietokannat ovat olleet pitkään MySQL, Oracle ja Microsoft SQL Server, jotka ovat kaikki SQL-mallia (Structured query language). SQL:ssä data tallentuu sarakkeisiin ja riveille. Tämä strukturoitu eli tiukan rakeenteen sisältävä tyyppi vaatii datan määrittämisen ennakkoon ennen sen viemistä tietokantaan. Strukturoidussa tietokannassa alkaa esiintyä ongelmia skaalautuvuudessa ja nopeudessa, kun datamassa kasvaa merkittävän suureksi. (Collin & Saarelainen 2016, 196.)

Erittäin tiukan rakenteen omaavan SQL-tietokannan sijasta voidaan käyttää NoSQL-tietokantaa, joka on paljon joustavampi ja hyvin skaalautuva. NoSQL-tietokanta on strukturoimaton ja tietovarastoon voi viedä sekalaista dataa ilman luokittelua ja pilkkomista

eri lokeroihin. Sekalaista dataa ovat esimerkiksi valokuvat, äänitiedostot, videot, tekstiasiakirjat ja mittausdata, joita voi syntyä hyvin erilaisilta sensoreilta. NoSQL tietovarastoon on kuitenkin pakko liittää jokin rakenne, jotta datatietueen voi löytää tietokannasta hauilla. Strukturoimaton tietovarasto on paljon ystävällisempi ohjelmoimiseen ja muutosten tekemiseen, koska datan rakenteen voi määritellä vasta jälkikäteen. NoSQL:n päällä on myös mahdollista käyttää SQL-rakennetta, joka voi helpottaa hakujen nopeutta. Markkinoiden suosituin (2015) NoSQL-tietokanta on MongoDB. (Collin & Saarelainen 2016, 196.)

4.5.2 Keskitetty tai hajautettu arkkitehtuuri

Keskitetyssä arkkitehtuurissa on yksi taustajärjestelmä, johon kootaan päätelaitteiden keräämä data. Taustajärjestelmä hallinnoi päätepisteitä ja rakentaa keskitetyt palvelut. Päätepisteet eivät ole tässä mallissa keskenään vuorovaikutuksessa. Päätepisteitä ovat esimerkiksi sensorit. (Collin & Saarelainen 2016, 201.)

Hajautettu arkkitehtuuri toimii kehittyneemmässä teollisessa internetissä, jossa päätepisteet ovat älykkäitä. Älykkäät päätepisteet voivat kommunikoida keskenään ilman keskitetyn järjestelmän jatkuvaa ohjausta. Eli P2P-vertaisviestintä on mahdollista. Hajautetussa järjestelmässä dataa voidaan prosessoida jo sen synty- ja kulutuspaikalla, joka mahdollistaa minimaalisen viiveen tietoliikenteeseen ja datan prosessointiin ja resurssien tehokkaamman käytön. (Collin & Saarelainen 2016, 201.)

4.5.3 Pilvipalvelu tietovarastona

Teollisen internetin tietovarasto on mahdollista tallentaa vaihtoehtoisesti myös ulkoiseen pilvipalveluun. Ulkoistettu tietovarasto pilvessä on edullinen ja hyvin skaalautuva vaihtoehto, koska omia fyysisiä palvelimia ja konesaleja ei tarvitse hankkia. Teollista internetiä varten suunnitellut pilvipalvelut omaavat myös datavaraston lisäksi analytiikan, laitehallinnan ja visualisointiin tarvittavat työkalut. (Collin & Saarelainen 2016, 202.)

Pilvipalvelu ei kuitenkaan aina sovi kaikissa tapauksissa yrityksen tietovarastoksi. Jos data on hyvin arkaluontoista, voi syntyä tietoturvaongelmia. Lisäksi pilvipalvelu aiheuttaa pakostikin latenssia ja verkkoyhteyden katkeaminen on mahdollista. Tämä ei sovi kriittisiin palveluihin, joissa pitää reagoida reaaliajassa esimerkiksi laitteiden rikkoutumisiin. (Collin & Saarelainen 2016, 202.)

4.6 **Analytiikka**

Sensoreiden keräämästä suuresta datamassasta saadaan hyöty irti vasta analysoimalla kerättyä dataa analytiikan työkalujen avulla. Analytiikan tarkoitus on olla tukena organisaation päätöksenteossa kaikilla tasoilla, tuottaa lisäarvoa liiketoiminnalle ennustemalleilla ja parantaa yrityksen toiminnan tehokkuutta ja laatua. Analytiikalla datamassasta voidaan seuloa poikkeavuudet ja trendit, jotka tuodaan esiin ymmärrettävässä muodossa visualisoinnin avulla. Datan analysoinnilla halutaan löytää informaatiota asetetun pohjaoletuksen tueksi, mutta analytiikka voi johtaa myös hypoteesin kumoamiseen ja näin voi syntyä uusi johtopäätös, jonka mukaan tuote, palvelu, teknologia tai koko liiketoimintamalli voi muuttua. (Collin & Saarelainen 2016, 205.)

Analytiikalla voidaan kuvailla mitä halutussa kohteessa, kuten esimerkiksi laitteessa on tapahtunut. Tapahtumia tuodaan esiin raporttien, hälytyksien, tai kartoituksien avuilla. Kuvailuista saadaan diagnostiikkaa tapahtumasta ja vastaus miksi jokin tapahtuma on tapahtunut. Diagnostiikka suoritetaan kyselyillä, datan louhinnalla tai tilastollisella analyysilla. Diagnostiikan perusteella tapahtumia pystytään jatkossa ennakoimaan ja ennustamaan mitä tulee tapahtumaan. Tapahtumia ennakoimalla toimintaa on mahdollista ohjata haluttuun päämäärään optimoinnilla ja suunnittelulla. (Collin & Saarelainen 2016, 205.)

Datamassan rajattoman suuresta koosta johtuen datan manuaalinen analyysi on todella hidasta ja työläistä, miltei mahdotonta. Analytiikassa käytetään automaattisia algoritmeja. Automaattiset algoritmit ajetaan laitetasolla, ja datan tulkinta jätetään älykkäille laitteille. Analysoitava datamassa voidaan jakaa kahteen osaan, jotka ovat: kerätty ja tallennettu data tai liikkeessä oleva data. Kerättyä ja tallennettua dataa eli lepäävää dataa tutkitaan rauhassa ajan kanssa analyysia varten, kun taas liikkeessä olevan datan tutkiminen mahdollistaa reaaliaikaisen analyysiin. (Collin & Saarelainen 2016, 205.)

Datamassan analysointi on mahdollista jättää kokonaan pilvipalvelun huolehdittavaksi, koska ne sisältävät usein tarvittavat työkalut analyysia varten. Kuitenkin analytiikka pyritään nykyään useammin suorittaa lähempänä datan syntypaikkaa ja tuottaa tietovarastoon laadukkaampaa dataa ja pienentää kaistan kuormitusta. Menetelmästä käytetään nimeä edge computing, jossa datan analysointi toteutetaan tietokoneohjaimien qpu-suurteholaskennalla, gateway-laitteilla tai sensoreiden prosessoreilla. (Collin & Saarelainen 2016, 205.)

Analytiikan menetelmiä on monia, mutta esittelen tässä opinnäytetyössä seuraavat menetelmät: koneoppiminen, rinnakkaisprosessointi ja muisti- ja virtausprosessointi.

4.6.1 Koneoppiminen

Koneoppiminen on tietojenkäsittelytieteen ala, jossa tietojärjestelmillä on kyky "oppia" datan avulla ilman erillistä ohjelmointia. Koneoppiminen voi olla tärkeä menetelmä teollisen internetin kannalta, koska tämä menetelmä mahdollistaa ennustusmallien luomisen esimerkiksi laitteiden vikaantumisista. Koneoppimisessa tarkoituksena on kirjoittaa algoritmeja, jotka ajetaan tarkasteltavaa dataa vastaan. Koneet oppivat algoritmien

avulla ympäristöstään jotakin, ja pystyvät tekemään datan avulla itsenäisesti ratkaisuja. (Collin & Saarelainen 2016, 210.)

Oppimismenetelmiä on tässä menetelmässä kolme erilaista: ohjattu oppiminen, vahvistusoppiminen ja ohjaamaton oppiminen. Ohjatussa oppimisessa tiedetään ennalta, mitä järjestelmä osaa lopputilanteessa. Algoritmi oppii tunnistamaan datasta hyvän ja pahan, ja tätä mallia käytetään luomaan ennustusmalli, joka kykenee hälyttämään ajoissa vikaantuvista laitteista. (Collin & Saarelainen 2016, 210.)

Vahvistusoppiminen on vuorovaikutusta, jossa algoritmia kiitetään hyvistä ratkaisuista ja moititaan huonoista. Algoritmia opetetaan siis palautteen avulla, jonka pohjalta se luo itselleen logiikan toiminnan ohjaukseen. Vahvistusoppiminen on käytössä robotiikassa, teollisen internetin kannalta sitä sovelletaan älykkäissä tehtaissa. (Collin & Saarelainen 2016, 210.)

Ohjaamaton oppiminen on menetelmistä haastavin, koska siinä datasta ei tiedetä ennalta mitään. Luotu algoritmi etsii datamassasta rakenteita, joilla löydetään datasta samankaltaisuuksia ja luodaan dataluokkia. Menetelmän välineitä ovat esimerkiksi klusterointi, itseorganisoituvat kartat ja neuroverkot. Ohjaamatonta oppimista voidaan soveltaa muun muassa anomalioiden tunnistamiseen, jotka saattavat ennakoida tulevaa vikaantumista. (Collin & Saarelainen 2016, 210.)

4.6.2 Rinnakkaisprosessointi

Rinnakkaisprosessoinnissa dataa käsitellään klusterissa. Klusterin sisältämät useat eri noodit toteuttavat samaa tehtävää samanaikaisesti laitejoukossa. Suurta määrää dataa voidaan käsitellä näin todella nopeasti, koska datan prosessointi voidaan jakaa koko klusterin laajuudelle. Rinnakkaisprosessointi ei kuitenkaan ole riittävän nopea menetelmä reaaliaikaiselle datan analysoinnille, jota teollinen internet tulee tarvitsemaan kriittisissä palveluissa. Reaaliaikaiseen analyysien tuottamiseen soveltuvat paremmin muisti- ja virtausprosessointi menetelmät. (Juurinen 2018.)

4.6.3 Muistiprosessointi

Muistiprosessointi menetelmässä data tallennetaan järjestelmän keskusmuistiin. Tämä menetelmä takaa nopean datan käsittelyn ja tuloksien esille tuonnin. Datan lukeminen keskusmuistista on jopa sata kertaa nopeampaan kuin levyn pinnalle tallennettaessa. Kuitenkin haittapuolena tässä menetelmässä on, että muistin määrän tarve kasvaa sitä mukaan, kun datan määrä kasva. Muistiprosessointi sopii hyvin reaaliaikaiseen analyysien tuottamiseen. Muun muassa aikaisemmin mainittu MongoDB-järjestelmä käyttää muistiprosessointimallia. MongoDB perustui ei-strukturoituun dataan, joten data voi sisältää myös puhetta tai valokuvia, jolloin myös analytiikan työkaluina täytyy olla kielen prosessointia ja hahmon tunnistusta. (Collin & Saarelainen 2016, 210.)

4.6.4 Virtausprosessointi

Virtausprosessointi toimii jopa vielä nopeammin analysoinnissa kuin muistiprosessointi, koska analysointi tapahtuu reaaliajassa. Virtausprosessoinnissa on käytössä SIMD-malli, jossa useat eri datalähteet suorittavat yhtä komentoa samanaikaisesti. Data tutkitaan tällä menetelmällä jatkuvilla kyselyillä suoraan datavirrasta esimerkiksi sensorien verkostosta ennen kuin data ehtii saapua tietokantaan. Virtausprosessointia käytetään hyödyksi paljon finanssialalla pörssikauppaan liittyen. (Juurinen 2018.)

4.7 **Tietoturva**

Luotettavan tietoturvan takaaminen teollisen internetin käyttöönottavalle yritykselle on todella suuri haaste, koska hyökkäyspinta-ala voi olla käsittämättömän suuri. Teollisen internetin luottamuksen edellytys on laitteiden ja verkkojen suojaaminen tietoturvariskeiltä. Käytännössä tämä tarkoittaa yhteyksien salaamista koneiden välisessä tietoliikenteessä, sulautettuja tietoturvaohjelmistoja ja käyttöoikeuksien hallintaa. (Lehto 2015). Tietoturva tulee huomioida kaikilla tasoilla, tarkoittaen teknologiapinossa alhaalta sensoritasosta aina huipulle liiketoimintaan saakka.

Luotettavan tietoturvan toteutumista hankaloittaa merkittävästi todella suuri laitteiden määrä, heterogeeniset IoT-järjestelmät, ulkopuoliset sidosryhmät ja työntekijöiden mahdolliset huolimattomuusvirheet. Heterogeeniset IoT-järjestelmät aiheuttavat tietoturvan kannalta tietoturvariskejä, koska tietoturvan ammattilaisilla on monia eri käyttöjärjestelmiä tai eri laitevalmistajien laitteita käytössä, ja he eivät ole aina perillä jokaisen eri käyttöjärjestelmän tai laitteiston kaikista tietoturvapuutteista. (Pervilä 2018.) Tilannetta ei myöskään helpota, että perinteiset teolliset hallinta- ja automaatiojärjestelmät ovat olleet alun perin tietoturvaltaan kevyitä, koska suljettuja järjestelmiä ei ole ajateltu liitettävän internetiin.

Yksi suurimmista ongelmista on että, enemmistö tietoturvan vastuuhenkilöistä ei edes tiedä järjestelmään yhdistettyjen laitteiden määrää (Pervilä 2018). Turvallinen IoT-järjestelmä riippuu paljon suunnittelusta, integraatiosta ja toteutuksesta. Ensinnäkin kartoitetaan koko järjestelmä ja tiedetään mitä verkkotopologian kaikki järjestelmät ja laitteistot pitävät sisällään, kuten mitä eri verkkoyhteyksiä (4G, Bluetooth, SigBee) laitteiden välillä käytetään. Lisäksi laajamittainen dokumentointi tietoturvasta ja verkon auditointi ovat olennaisia keinoja pysyä kartalla verkon tapahtumista. (Collin & Saarelainen 2016, 245.)

Tietoturvauhkia käsitellään vielä uudestaan kappaleessa IoT:n hyödyt ja haasteet.

5 IOT HYÖDYT JA HAASTEET

5.1 Hyödyt

IoT:n tuomia hyötyjä voidaan tarkastella erikseen yritysten, yhteiskunnan ja kuluttajien näkökulmista. Verkkoon kytketyt älykkäät laitteet ja palvelut tuovat erilaisia hyötyjä eri näkökulmista katsottuna. Yritykset hyödyntävät teollista internetiä pääosin tehostamalla nykyistä liiketoimintaa, luomalla kokonaan uutta liiketoimintaa tai kasvattamalla tuotteiden arvoa. Yhteiskunta hyötyy IoT:sta tietoyhteiskunnan kehittymisen kautta, kun syntyy uusia integroituja digitaalisia palveluja. Kuluttajat taas hyödyntävät esineiden internetiä arkisien tarpeiden tyydyttämiseen. (Juhanko ym. 2015, 20-29.)

Yrityksien liiketoiminnan tehostaminen perustuu älykkäiden laitteiden, koneiden ja prosessien keräämän datan tehokkaampaan hyödyntämiseen. Hyöty yrityksille voi syntyä ennakoivan huollon, energian säästön tai työvoiman tehokkaamman käytön ansiosta. Tehokkaalla toiminnalla säästetään yrityksien kuluja ja liiketoiminnalle saadaan parempi kate. Yritykset säästävät esimerkiksi ennakoivalla huollolla turhia huoltotoimenpiteitä tarkan oikean ajoituksen vuoksi ja rakennuksissa ja kulkuneuvoissa voidaan säästää energiaa muun muassa optimaalisella valaistuksella, lämmönjakelulla ja polttoaineen käytöllä. (Juhanko ym. 2015, 22.)

Uutta liiketoimintaa syntyy, kun siirrytään pelkästä tuotteiden valmistamisesta ja myymisestä niiden palveluliiketoimintaan. Palvelu sisältää huollon, operoinnin ja suorituskyvyn myynnin, joten toimittaja saa pitkäaikaset tulot, joita on helpompi ennakoida. (Juhanko ym. 2015, 22.) Tuotteiden ja palveluiden kehittäminen älykkäämmiksi kasvattavat tuotteiden arvoa uusilla ominaisuuksilla, lisääntyneellä asiakasräätälöinnillä ja paremmalla käytettävyydellä. Liiketoiminnan asiakasarvon nostaminen voi kasvattaa yrityksien liikevaihtoa ja kannattavuutta. (Quava 2017, 6.)

Yritykset tulevat hyötymään datamassojen keräämisestä, koska itsessään datasta on tulossa myytävä tuote, kauppatavaraa. Raakadatan myyminen voi synnyttää uutta liiketoimintaa, mutta vasta datan jalostus tekoälyn, IoT-teknologian tai koneoppimisen avulla mahdollistaa lisäarvon uuden liiketoiminnan kannattavuudelle. Datan jalostuksen loppumuotona voidaan pitää algoritmia, innovaatiota, joka voidaan suojata patentilla, ja yritykset voivat saada lisäarvoa liiketoiminnalle entisestään patenttien kautta. (Ahola ym. 2017, 12-15.)

Jalostetusta datasta syntyy tärkeää tietoa ja käytännön hyötyjä teollisen internetin mahdollisuuksia hyödyntävälle yritykselle. Yrityksen toiminnasta kertyvän datan analysoinnilla voidaan päätellä mitä tuotannon prosesseissa oikeasti tapahtuu ja löytää eri tekijöiden ja ilmiöiden yhtyvyydet. Ihmisen käsityskyky on rajallinen, joten analyyseilla saadaan parempi hahmotelma tuotannon kokonaiskuvasta. Tiedon jalostamiseen liittyvä automaatio lisää myös nopeutta ja tarkkuutta esimerkiksi vianselvitystilanteissa. Automaatio vähentää asiantuntijoiden rutiininomaisia työtehtäviä, joten asiantuntijan työajasta suurempi osa saadaan keskitettyä päätöksentekoon, joka perustuu uuteen jalostettuun tietoon. Laatuvirheiden ja tuotantohäiriöiden suhteen yrityksen toiminta muuttuu enemmän proaktiiviseksi, koska reaaliaikainen datan analysointi helpottaa toiminnan ennakointia. Lisäksi laitevalmistajat saavat jatkuvaa dataa ja tarkkaa tietoa

kuluttajien yksittäisten laitteiden käytöstä, jolloin yritys voi ymmärtää paremmin jalostetun tiedon perusteella asiakaskäyttäytymistä. Asiakaspalautteet eivät sisällä yhtä tarkkaa tietoa tuotteiden käytöstä, joten yrityksen pystyvät tarjoamaan parempaa huolto- ja käytönohjauspalvelua. (Ackerman ym. 2016.)

5.2 **Haasteet ja hidasteet**

IoT:n kehittämisen tiellä on vielä monia haasteita ratkaistavana. Suurin osa haasteista liittyy tietoturvaongelmiin, yksityisyyden uhkiin, puutteisiin yhteisissä standardeissa ja yrityskulttuurin muutokseen. Suurimmaksi hidasteeksi koetaan markkinoiden kypsymättömyys sekä osaamisen puute. (Arrow 2017.)

5.2.1 Teknologian, osaamisen ja yrityskulttuurin pullonkaulat

Teollisilla yrityksillä on puutteita laajasta asiantuntemuksesta koko teknologiapinon kannalta ja ICT-yrityksillä ongelmana on toimialan asiantuntemuksen puutteita oikeiden ratkaisujen tunnistamiseksi. Siirtyminen perinteisestä tuoteliiketoiminnasta teollisen internetin palvelu- ja informaatio-liiketoimintaan vaatii soveltamista uusien liiketoimintamallien ja liiketoimintamenetelmien kanssa. Esteinä ovat soveltamisen vaikeus liittyen uusien liiketoimintamallien turvallisuuteen, sopimuksiin ja vastuisiin. (Juhanko ym. 2015, 40.)

Tarvittava teknologia IoT:n etenemiselle on olemassa, mutta kilpailu standardeista ja alustoista on vielä kesken. Tiedonsiirtojen rajapintojen standardien puute on yksi suurimmista ongelmista ja moni yritys odottaa standardien ja toimintatapojen selkiytymistä ennen IoT:hen panostamista tosissaan. (Lindroos ym. 2016, 35.)

Nykypäivänä on mahdotonta rakentaa yksittäinen ja globaali älykkäiden esineiden toiminnallinen kokonaisuus, ekosysteemi, jossa älykkäät esineet kommunikoisivat saumattomasti. IoT-verkkoon liitetyillä laitteilla ja sovelluksilla ei ole universaalia "yhteistä kieltä", jolla voitaisiin verkkojen välillä kommunikoida riippumatta fyysisistä liitännöistä. Nykyaikainen esineiden internet koostuu periaatteessa kasvavasta kokoelmasta privaatteja verkkoja, jotka ovat eristettyjä, eivätkä verkot voi kommunikoida keskenään uniikin universaalin sovellusprotokollan puutteen vuoksi. (Guinard & Trifa 2016, 6.)

Monissa vanhoissa teollisuusyrityksissä on vielä suuri historian painolasti taakkana. Legacy-järjestelmät ja suuri vanha laitekanta hidastavat teollisen internetin kehitystä, vaikka monissa laitteissa onkin toiminnastaan ja ympäristöstään dataa keräämiä anturreita, mutta ongelmat liittyvät tiedonsiirtoon datan viemisestä ulos suljetuista järjestelmistä. Koko laitekannan modernisointi on massiivinen investointi, johon harvalla on edes mahdollisuutta, joten IoT:n kehitys laahaa laitekannan uusimisen tahdissa. (Lindroos ym. 2016, 36.)

Teollinen internet tuo muutoksia toimialojen toimintamalleihin, ja haasteena on opettaa uudet toimintatavat asiakkaille, jotka ovat tottuneet perinteisiin toimintamalleihin. Esimerkiksi huoltosopimuksien muutos tulee vähentämään laitehuoltajien käyntejä

paikan päällä. Uusien toimintamallien käyttöönottoa hidastavat rohkeus kokeilla uusia toimintatapoja ja vakiintuneiden toimintatapojen puutos. Asiakkaiden ostotapa täytyy kääntää laitteen omistamisesta laitteen käytön ostamiseksi palveluna. (Lindroos ym. 2016, 39.)

Teollisen internetin kehitys vaatii yrityksien välistä yhteistyötä ja verkostoitumista. IoT voi tuottaa uudenlaisia ekosysteemejä, kun suuret ja pienet yritykset alkavat liittyä yhteen ja toimimaan avoimemmin partnereina. IoT:n mahdollistama uudenlainen ajattelutapa voi murtaa vanhan perinteisen alihankkijamallin, jossa suuremmat yritykset määrittelevät pelisäännöt. Ekosysteemiajattelu vaatii syvempää luottamusta, tiiviimpää ja tasavertaisempaa yhteistyötä ja yhteistä tuotekehitystä. Nykypäivänä ei kuitenkaan olla vielä luottavaisia avoimuuden suhteen ja yritykset tahtovat säilyttää liikesalaisuudet talon sisässä, mikä jarruttaa ekosysteemiajattelun etenemistä. (Lindroos ym. 2016, 40-41.)

Monilta yrityksiltä puuttuu vielä strategia datan suhteen ja vieroksutaan ajatusta datan vaihtamisesta ja yhdistämisestä yli yritysrajojen. Kuitenkin yritykset tiedostavat datan hyödyntämisen merkityksen ja ovat halukkaita kehittämään datan pohjalta uutta liiketoimintaa. Suomalaiset yritykset näkevät vielä datan keräämisen hyvin perinteisellä tavalla ja perustavat sen pelkästään omiin sovelluksiin ja sosiaalisen median lähteisiin. Asiakastietoja ei kerätä vielä ulkopuolista sovelluslähteistä. Dataliiketoimintaan siirtyminen edellyttää, toimintakulttuurin ja ajatusmallien muutosta, mutta riskiä ei uskalleta ottaa, koska dataan pohjautuvan liiketoiminnan tulevaisuutta ei osata ennustaa vielä tarkasti. (Ahola ym. 2017, 18-19.)

5.2.2 Tietoturva ja yksityisyys

Esineiden internetin kasvu luo haasteita tietoturvalle. Tietoturva puutteita ilmenee niin yrityksien verkoissa, kuin myös kuluttajille tarkoitetuissa laitteissa. Tietoturvapuutteita käytetään hyödyksi muun muassa toiminnan haittaamiseen ja häirintään, vakoiluun ja henkilökohtaisten tietojen urkintaan ja kiristämiseen rahallisen hyödyn tavoittelemiseksi. IoT:n tuomia erilaisia riskejä ja uhkia liittyen tietoturvaan ja datan hallinnointiin voidaan tarkastella myös yrityksien, yhteiskunnan ja kuluttajien näkökulmista. (Viestintävirasto 2018, 19-21.)

Yrityksien välillä on kova armoton kilpailu ja teollista internetiä voidaan käyttää yritysvakoiluun. Kilpaileva yritys haluaa saada selville liikesalaisuuksia hyödyttämään omaa toimintaansa. Yrityksen järjestelmään murtautuminen vaarantaa koko yrityksen sisäisen verkon, etäkäytettävät automatisoidut laitteet ja palvelimet. Hyökkääjä voi saada käsiinsä yrityksen salaisia piirustuksia, henkilöstötietoja ja liikesalaisuuksia. (Vieno 2015.)

Yhteiskunnalle IoT tuo uhkakuvia kriittisiin järjestelmiin, joita ovat esimerkiksi terveydenhuollossa, energiatuotannossa ja sähköverkoissa. Valtiolle voidaan aiheuttaa vakavaa haittaa murtautumalla kriittisiin järjestelmiin. Yksi räikeimmistä esimerkeistä on Stuxnet mato, joka levisi Iranin ydinlaitoksiin, vaikka järjestelmät olivat eristettyjä Internetistä. Tämä tietokonemato aiheutti suurta vahinkoa Iranin ydinohjelmalle. Suo-

messa kyberturvallisuuskeskus järjestää säännöllisesti suojaamattomien automaatiolaitteiden ja -järjestelmien kartoitusta. Havaintojen avulla kriittisten järjestelmien omistajat ovat saaneet tiedon suojauksen tarpeesta ja ryhtyneet toimenpiteisiin. (Viestintävirasto 2018, 19-21.)

Kuluttajille suunnattu esineiden internet on nykyisellään huomattava uhka riittämättömien turvallisuutta ja käyttöä koskevien määräyksien puutteen vuoksi. Kuluttajille tulee paljon uusia laitteita arkikäyttöön puettavan teknologian ja älykodinkoneiden muodossa. Kuitenkin monissa tapauksissa uutta tekniikkaa ajetaan nopeasti ihmisten käyttöön välittämättä kuluttajien yksityisyydestä tai datan suojaamisesta. (F-secure n.d.). Älykkäiden laitteiden tietoturvapuutteet altistavat hakkeroinnille ja niitä voidaan käyttää osana laajempia palvelinestohyökkäyksiä tai yksittäisten henkilöiden vakoiluun. Yksittäistä henkilöä on mahdollista seurata tai kuunnella, riippuen mitä tekniikka saastunut laite sisältää. (Viestintävirasto 2018, 19-21.)

6 **POHDINTA**

IoT on kovaa vauhtia kehittymässä eteenpäin osana digitalisaatioita. IoT:n todellinen hyödyntäminen alkaa näkyä käytännössä oletettavasti muutaman vuoden sisään, kun tehdään läpimurtoja suurimpien käyttöönottoon vaikuttavien hidasteiden kanssa. Esimerkiksi ratkaistaan kilpailu tiedonsiirron rajapintojen standardien välillä, nähdään mihin 5G-verkko kykenee käytännössä ja uuden teknologian hinta laskee suotuisaksi investoinneille. Älykkäät esineet alkavat myös yleistyä katukuvassa ja ihmisien kotona, kun uusia innovaatioita pusketaan markkinoille hyödyttämään arjen askareissa.

Kun Internet yleistyi ja levisi ympäri maailmaa lähes kaikkien ihmisien ulottuville, voitiin huomata ajatuksien ja tiedon leviämisen nopeuden räjähdysmäinen kasvu. Siinä missä Internet yhdisti ihmiset, tulee IoT yhdistämään älykkäät esineet ja järjestelmät globaalisti, ja tarjoaa ihmisille todella paljon tarkkaa ja reaaliaikaista dataa tukemaan päätöksiä. IoT tulee tehostamaan toimintaprosesseja aina yksittäisestä tehtaan tuotantolinjasta tai kerrostalon ihanteellisesta lämmön ja valaistuksen sääntelystä aina kokonaiseen älykaupunkiin asti. Tehokkaampi toiminta tulee näkymään resurssien säästönä, joka vähentää kulutusta ja turhaa työtä. Toisaalta tietotekniikan lisääntyminen lisää tietotekniikan valmistamiseen tarvittavien arvokkaiden raaka-aineiden tarvetta.

Suomi on lähtenyt hyvin mukaan teollisen internetin kehittämiseen ja sen luomien mahdollisuuksien hyödyntämiseen, vaikka onkin vielä teknologian käyttöönotossa lapsen kengissä. Suomi ei ole kuitenkaan pysynyt IoT:n edelläkävijämaiden USA:n, Saksan ja Kiinan vauhdissa kehityksessä. Tähän on vaikuttanut varmasti Suomen pienet markkinat, mutta luultavasti myös suomalaisten yrityksien puute rohkeudessa investoida kunnianhimoisiin IoT-hankkeisiin.

Esineiden internet tulee todennäköisesti hyödyttämään ja helpottamaan kuluttajien elämää erilaisilla sovelluksilla, mutta älyn lisääminen kaikkiin mahdollisiin esineisiin herättää kuitenkin vielä paljon kysymyksiä: Kuinka paljon lisää haluamme informaatiota

ulottuvillemme, kun jo nyt älypuhelimien yleistymisen jälkeen on puhuttu ns. tietoähkystä? Mihin kaikkiin esineisiin sensoreita tarvitsee oikeasti lisätä? Pusketaanko uutta teknologiaa väkisin ihmisien arkeen taloudellisista syistä, ottamatta huomioon terveyteen ja yksityisyyteen liittyviä riskejä?

Suurimmalla osalla kuluttajista ei ole käsitystä mihin kaikkeen älykkäät esineet kykenevät. Esimerkiksi jopa älytelevisio voi tallentaa meistä ääntä tai videota valmiustilassa (Vänskä 2017). Esineiden internet tuo uusia mahdollisuuksia kuluttajien laitteiden hakkerointiin ja vakoiluun, ja viime aikaisien suurien paljastuksien takia ei voida olettaa, että tiedustelupalvelut keräävät dataa vain rikoksiin epäillyistä. Kuluttajien yksityisyys on entistä uhatumpi, kun älykkäät esineet tulevat osaksi arkielämää.

Euroopassa noudatetaan usein varovaisuusperiaatetta, jolla tarkoitetaan, että kuluttajien keskuuteen leviävät tuotteet pitää ensin todistaa terveydelle vaarattomiksi. Kuitenkin useat tutkijat varoittavat 5G-teknologian tuomasta lisääntyvästä säteilystä (Ahtela 2017). Tutkijoiden varoituksista huolimatta 5G-teknologia on tulossa lähiaikoina ja sen aiheuttamista terveysvaikutuksista saamme todennäköisesti lukea vasta tulevaisuudessa. IoT:n taloudellista potentiaalia ennustetaan niin kovaksi, että se menee mahdollisten terveyshaittojen edelle.

LÄHTEET

Ackerman, E., Collin, J., Martinsuo, M., 2016. Teollinen internet: Avain tietoon, uudistumiseen ja palveluliiketoimintaan. Promaint 17.3.2016. Viitattu 24.4.2018 https://promaintlehti.fi/Tuotantotehokkuuden-kehittaminen/Teollinen-internet-Avain-tietoon-uudistumiseen-ja-palveluliiketoimintaan/(offset)/28

Ahola, P., Harra-Salonen, K., Kiviluoto, K., Nummi, J., Olkkonen, J., Onniselkä, K., Parvinen, P., Seppälä, T., Sulin, K., Ääri, V-P. 2017. Datavallankumous ja liiketoiminta. Think Tank Teollinen internet ja IoT. Solita Oy. Viitattu 24.4.2018 https://www.solita.fi/think-tank

Ahtela, K. (2017) Tutkijat varoittavat: 5G verkko on terveysriski, EU:n lykättävät rakentamista. *Kauppalehti.* Viitattu 27.4.2018. https://www.kauppalehti.fi/uutiset/tutkijat-varoittavat-5g-verkko-on-terveysriski--eun-lykattava-rakentamista/4yAEFs2a

Ailisto, H.(toim.), Mäntylä, M.(toim.), Seppälä, T.(toim.), Collin, J., Halén, M., Juhanko, J., Jurvansuu, M.,Koivisto, R.,Kortelainen, H.,Simons, M.,Tuominen, A. &Uusitalo, T. 2015. Suomi –Teollisen Internetin Piilaakso. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 4/2015. Viitattu 6.4.2016

Arrow. 2015. IoT-matka. Internet of Things on mahdollisuus. Arrow ECS. Viitattu 20.3.2017. http://iotfinland.fi.

Arrow. 2017. IoT:n tila Suomessa – barometri 2017 ja vertailu 2015-2017. Arrow ECS. Viitattu 20.3.2017. https://docs.wix-static.com/ugd/33307d_50ba8c6abd6c4b96abf04c8c5d00aa93.pdf

Ashton, K. (2009). That 'Internet of Things' Thing. Blogijulkaisu 22.6.2009. Viitattu 15.3.2017. http://www.rfidjournal.com/articles/view?4986

Collin, J., Saarelainen, A. 2016. Teollinen internet. Talentum. Helsinki 2016.

F-Secure (n.d.) Pinning Down the IoT. Cyber Security Research Institute report into the Internet of Things. Viitattu 25.4.2018. https://fsecureconsumer.files.wordpress.com/2018/01/f-secure_pinning-down-the-iot_final.pdf

Guinard, D., Trifa, V. 2016. Building the Web of Things. Manning. 2016.

Lehto, T. (2016) Kännykät, tehkää tilaa! – Iot-laitteet vilahtivat suosion huipulle. *Tekniikka&Talous.* Viitattu 27.4.2018. https://www.tekniikkatalous.fi/tekniikka/kannykat-tehkaa-tilaa-iot-laitteet-vilahtivat-suosion-huipulle-6595229

Hänninen, K. (2017) Suomi on älyteknologian ja teollisen internetin huippuhyödyntäjä. *Tekniikka&Talous.* Viitattu 24.4.2018. https://www.tekniikkatalous.fi/tekniikka/ict/suomi-on-alyteknologian-ja-teollisen-internetin-huippuhyodyntaja-6638077

Juhanko, J. (toim.), Jurvansuu, M. (toim.), Ahlqvist, T., Ailisto, H., Alahuhta, P., Collin, J., Halen, M., Heikkilä, T., Kortelainen, H., Mäntylä, M., Seppälä, T., Sallinen, M., Simons, M. & Tuominen, A. 2015. Suomalainen teollinen internet – haasteesta mahdollisuudeksi: taustoittava kooste. ETLA Raportit No 42. Viitattu 24.4.2018 https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-42.pdf

Juurinen, S. (2018). Big data –teknologia perusteet ja mahdollisuudet. Opinnäytetyö. Tuotantotalous. Metropolia ammattikorkeakoulu. Viitattu 5.4.2018 http://urn.fi/URN:NBN:fi:amk-201304265249

Lehto T. (2015) Tietoturva ratkaisee teollisen internetin kohtalon. *Tivi.* Viitattu 23.4.2018. https://www.tivi.fi/Uutiset/2015-03-25/Tietoturva-ratkaisee-teollisen-internetin-kohtalon-3218046.html

Lindroos, O., Pirinen, V., Stenbäck, A., Aro, M., Penttinen, P., Pankakoski, J., Hagros, K. & Seppälä, T. 2016. Mikä jarruttaa IoT-kehitystä? Think Tank Teollinen internet ja IoT. Solita Oy. Viitattu 24.4.2018. https://www.solita.fi/think-tank

Pervilä, M. (2018) Iot:n tietoturva mättää, ja seuraukset ovat vakavia: ”Tämä ei ole enää teoriaa”. *Tivi.* Viitattu 23.4.2018. https://www.tivi.fi/CIO/iot-n-tietoturva-mattaa-ja-seuraukset-ovat-vakavia-tama-ei-ole-enaa-teoriaa-6698875

Quava. 2017. Yritysjohdon opas IoT:n ja teollisen internetin hyödyntämiseen. Elisa & Quava. Viitattu 23.4.2018 http://quva.fi/site/attachments/yritysjohdon_opas_IoT_ja_teollisen_internetin_hyodyntamiseen.pdf

Vieno, J. 2015. Teollinen internet ja tietoturva. Blogijulkaisu 1.12.2015. Viitattu 25.4.2018. https://www.v-tek.fi/teollinen-internet-ja-tietoturva/

Viestintävirasto. 2018. Tietoturvan vuosi 2017. Viestintäviraston julkaisu 001/2018 J. Viestintävirasto. Viitattu 25.4.2018 https://www.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Tietoturvan-vuosi-2017.pdf

Vänskä, O. 2017. Onko televisiosi hakkeroitu? Näin saat sen selville. *Tivi.* Viitattu 27.4.2018. https://www.tivi.fi/Kaikki_uutiset/onko-televisiosi-hakkeroitu-nain-saat-sen-selville-6631305