

Iiro Kuitunen

Anturista pilveen -tietoturva



Tradenomi
Tietojenkäsittely
Syksy 2018



KAMK • University
of Applied Sciences

Tiivistelmä

Tekijä(t): Kuitunen Iiro

Työn nimi: Anturista pilveen -tietoturva

Tutkintonimike: Tietojenkäsittelyn tradenomi, Datacenter

Asiasanat: Tietoturva, Internet of Things, mobiiliverkko, terveydenhuolto

Tämän opinnäytetyön tavoitteena oli kartoittaa Internet of Thingsin lukuisten verkkoprotokollien tilannetta niiden ominaisuuksien, tietoturvan ja tulevaisuusnäkökannalta. Tarkoituksena oli auttaa oikeiden protokollien valitsemisessa niille sopiviin tehtäviin, kuten terveydenhuollossa potilaan terveydentilan mittaamiseen, logistiikan alalla tavaroiden paikantamiseen tai tietoturvaliikkeen sensoridatan keräämiseen. Eri teknologioita arvioitaessa kiinnitin huomiota erityisesti tietoturvaan, mahdollisiin datamääriin, kantomatkaan, sekä energiatehokkuuteen. Otin myös tarkemman katsauksen DigiOS-projektin käyttämiin teknologioihin, kuten Bittiumin Tough Mobile -älypuhelimeen, projektin tietokantaratkaisuihin, sekä käytettäviin verkkoprotokollisiin.

Työssä ei ollut käytännön tehtävää, vaan se oli puhdas tutkimusprojekti, jossa etsin tietoa Internet of Thingsin erilaisten teknologioiden nykytilasta, tulevaisuusnäkökannasta, sekä tietoturvasta. Tietolähteinä käytin alan tutkimusten raportteja, alan verkkosivujen artikkeleita, asiantuntijoiden blogeja, sekä yritysten ja yhteisöjen keräämiä tietokokoelmia ja markkinointimateriaaleja. Parhaita tietolähteitä oli tietoturvan ja IoT:n asiantuntijoiden ja tutkijoiden aiheeseen pureutuvat tutkimukset ja raportit, mutta eniten löytyi erilaisia yleiskatsauksia, sekä lyhyitä verkkojulkaisuja, joissa aihetta ei käsitelty pintaa syvemältä. Tällaisissa tilanteissa täytyi samasta aiheesta löytää verrattavia artikkeleita muualta, jotta sain karsittua markkinoinnin hypeä oikean tiedon ympäriltä pois. Joissain tapauksissa tietoa piti myös hakea teknologiaa kehittävä tahon omilta sivuilta tai materiaaleista, jos ulkopuolista tutkimusta ei ollut saatavilla. Tällaiseen tietoon suhtauduin varauksella, sillä yritykset haluavat myydä omaa tuotettaan, eikä kaikilta aina ollut tarjolla todisteita esittelemistä ominaisuuksistaan.

Työssä opin, että IoT:n alalla on valtava määrä enemmän ja vähemmän toistensa kanssa kilpailevia teknologioita. Tämä johtuu siitä, että IoT kattaa laajan alan eri käyttötarkoituksia, joihin vaaditaan laitteilta ja teknologioilta eri ominaisuuksia. Hyvän energiatehokkuuden ja pitkän akunkeston aikaansaamiseksi jokin teknologia on voinut leikata mahdolliset datamäärät erittäin pieniksi. Hyvää turvallisuutta painottava teknologia on saattanut kehittää kokonaan oman teknologiansa, mutta samalla karsinut yhteensopivuutta muiden laitteiden kanssa. Oikean ratkaisun löytäminen vaatii projektin toteuttajilta hyvää suunnittelua, vaatimusten kartoittamista, sekä tietoturvan kohdalla hyvää riskienhallintaa. Kokonaisen järjestelmän tietoturvan takaaminen vaatii asiantuntijoilta yleiskuvan hahmottamista, sekä jokaisen laitteen ja teknologian kohdalla syvempää tietoturvaosaamista, sillä erityisesti tietoturvan toteuttamiseen ei ole oikoreittejä.

Abstract

Author(s): Kuitunen Iiro

Title of the Publication: Sensor-to-cloud information security

Degree Title: Bachelor of Business Information Technology, Datacenter

Keywords: Information Security, Internet of Things, mobile network, healthcare

The objective of this thesis was to research the various Internet of Things network protocols, their current usage and their projected future headings. This helps with choosing the right protocols for different IoT tasks like medical monitoring, GPS location tracking or secured data collecting. The main focuses when classifying different of protocols were their current information security standings, the protocols challenges, future, and performance in the form of data bandwidth, operating range and energy efficiency. I also took a closer look into the technologies used in the DigiOS project and analyzed possible points of security hardening. This included Bittium's Tough Mobile smartphone, the monitoring devices, databases and the connections for all these technologies.

The thesis didn't have a practical task as it was purely a research into the security and Internet of Things industry. The research was conducted using publicly available research papers, written articles and different kinds of news releases and marketing material. The best information sources were white papers by industry experts and researchers but most of the information came from comparing different sources, for example newspapers, magazines and technology journals to filter out as much marketing hype as possible. This was especially difficult in cases where the only available information sources were the people developing the protocol or system themselves. Sometimes even they didn't provide any solid backup for their claims and in such cases I had to make a point to analyze any information with a pinch of salt.

What I learned from the thesis is that the Internet of Things industry is far from standardized. There's such a large variety of use cases for small monitoring devices that a single solution for everything is impossible at the moment. However, this makes choosing the right device and connection type difficult because every one of them has their pros and cons. One could have a solid range with good transfer speeds but consume much more electricity than its competitors. Another might have a solid security base and be really energy-efficient but only allow tiny amounts of data at a time. Finding the right combination of technologies for the job requires analyzing the project needs and comparing them to the current and upcoming solutions. When it comes to Internet of Things, security is often the lackluster part of the system. In many cases the developers left the responsibility of securing the system for the people implementing it. It also means that when security is a concern in a larger project, risk assessment should be conducted by professionals.

Sisällys

| | | |
|-------|---|----|
| 1. | Johdanto | 1 |
| 2. | IoT:n kasvu ja tietoturva | 3 |
| 3. | IoT-järjestelmät | 5 |
| 3.1 | IoT-laite..... | 5 |
| 3.2 | Yhteydet | 6 |
| 3.3 | Vastaanottaja | 6 |
| 3.4 | Standardisoinnin tarve | 7 |
| 4. | Yhteysprotokollat ja standardit | 8 |
| 4.1 | WiFi..... | 8 |
| 4.2 | Bluetooth ja BLE | 9 |
| 4.3 | Matkapuhelinverkko | 10 |
| 4.3.1 | 4G LTE..... | 11 |
| 4.3.2 | 3G ja 2G | 12 |
| 4.4 | ZigBee | 13 |
| 4.5 | Z-Wave..... | 13 |
| 4.6 | Sigfox | 14 |
| 4.7 | NFC | 15 |
| 4.8 | LTE Cat. M1, 0, EC-GSM, NB-IoT ja 5G..... | 16 |
| 4.9 | Thread | 17 |
| 5. | Case: DigiOS..... | 19 |
| 5.1 | BLE | 20 |
| 5.2 | Bittium Tough Mobile..... | 21 |
| 5.3 | SafeMove..... | 22 |
| 5.4 | Gillie.io, MQTT | 22 |
| 5.5 | MySQL, NoSQL..... | 25 |
| 5.6 | Terveydenhuollon vastuhenkilö..... | 25 |
| 6. | Yhteenveto | 27 |
| | Lähteet | 28 |

standardia käyttävien asioiden kanssa. Vrt. protokolla, joka on standardia tarkempi määritelmä esimerkiksi siitä, miltä jokin verkkoliikenteen paketti tulisi näyttää.

TLS / SSL – Transport Layer Security / Secure Socket Layer, eli tietoverkkojen salausprotokolla. Etenkin web-sivuilla oleva salaus on usein tehty käyttäen TLS- tai SSL-salausta. Salaukseen kuuluu joko itse tehty, tai ulkopuoliselta taholta hankittu salainen salausavain, jota käyttämällä yhteys salataan. Useimmat sivustot hankkivat salausavaimet ulkoisilta, luotetuilta salausavainten tarjoajilta. Tarkoituksena on todentaa sivuston identiteetti oikeaksi.

VPN – Virtual Private Network, eli virtuaalinen erillisverkko. Yksityinen salattu tai tunneloitu verkkoratkaisu, joka mahdollistaa kahden tai useamman järjestelmän keskustelun, kuin ne olisivat samassa verkossa.

1. Johdanto

IoT, Internet of Things, eli esineiden ja asioiden internet on internetin laajentumista normaaleista tietokoneista erilaisiin koneisiin, laitteisiin ja sensoreihin. Terminä IoT:tä on käytetty jo pitkään, mutta sen nopea leviäminen ja kasvu 2010-luvulla on saanut monet tahot valtioista suuryrityksiin ottamaan käyttöön erilaisia sitä hyödyntäviä käytännön sovelluksia. Se on merkittävä tekijä jo nykyisissä tietoverkoissa, mutta vielä enemmän tulevaisuudessa, sillä henkilökohtaisten laitteiden, kuten sykemittareiden lisäksi erilaisia mittareita pystytään käyttämään monenlaisiin asioihin tulipaloista hälyttämisestä kasvien tarkkailuun ja kasteluun.

Aikaisemmin pienempien laitteiden kytkeminen verkkoon on ollut haasteellista virrankulutuksen takia, sillä virtaa tarvitseva laite tarvitsee väistämättä akun tai seinäpistokkeen tai muun vastaavan virtalähteen, eikä tarpeeksi kestäviä pieniä virransyöttöratkaisuja ollut saatavilla. Akkujen ja virtajohtojen tuomien ongelmien lisäksi päänvaivaa toi yhteyden toteuttaminen. Jokaiseen pieneen anturiin ei haluttu erikseen tuoda Ethernet-johtoa, joten langaton toteutus oli tarpeen. Langattomat verkot toivat mukanaan lisää virrankulutusta verrattuna langalliseen yhteyteen.

Tekniikan kehittyessä langattomat standardit ovat tavoitelleet näiden ongelmien pienentämistä ja mitätöimistä. Laitteiden energiatehokkuutta parannetaan jatkuvasti, jotta niitä voidaan käyttää samalla paristolla tai akulla pidempään vaihtamatta virtalähdettä. Samalla myös virtalähteitä kehitetään entistä energiatehokkaammiksi. Laitteissa käytettäviä ohjelmistoja ja protokollia on suunnattu enemmän IoT:n vaatimuksia kohti esimerkiksi tekemällä niistä mahdollisimman kevyitä pienten laitteiden hyvin rajallisen suorituskyvyn vuoksi.

Nyt teknologia on kehittynyt tarpeeksi pitkälle, että IoT:n käyttöön pystytään keskittymään enemmän. Riippuen käyttötarkoituksesta tämä voi tarkoittaa käyttötavan suunnittelua ja hiomista tai aikaisempien suunnitelmien ja ideoiden tuomista käytäntöön. Koska IoT-laitteet ovat monesti jollain yhteydellä kiinni laajemmassa verkossa, halutaan niiden tietoturvaan myös puuttua, sillä niitä on käytetty hyväksi laajojen verkkohyökkäysten, kuten Mirai-bottiverkon toteuttamiseen. Siinä löysästi suojattuja IoT-laitteita käytettiin DDoS-hyökkäysten voimavarana. Tämänlainen DDoS-hyökkäys toimii käytännössä siten, että hakkeroitu IoT-laite lisätään lukuisten muiden laitteiden kanssa bottiverkkoon, joka ohjataan pommittamaan verkossa paketteja yksittäistä tietokonetta tai verkkolaitetta, jolloin oikeiden käyttäjien liikenne hidastuu tai katkeaa, tai käytössä olevat verkkolaitteet hajoavat tai jumiutuvat. IoT-laitteiden ja ohjelmien kehityksessä tehdyt parannuk-

set esimerkiksi suorituskykyyn ja virrankulutukseen ovat monen laitteen kohdalla johtaneet siihen, ettei niiden tietoturva ole korkealla tasolla. Näiden laitteiden suorituskyky ei myöskään riitä ylläpitämään tietoturvaohjelmistoa itse laitteessa, joten tietoturva tulee hoitaa esimerkiksi verkon puolella. IoT:n tuominen alueille, joissa laitteet halutaan pitää tietoturvaisina, on aiheuttanut viime vuosina keskustelua, sillä sen tuomat mahdollisuudet esimerkiksi hoitoalalla, jossa käsitellään hyvin arkaluontoista tietoa, houkuttelevat monia.

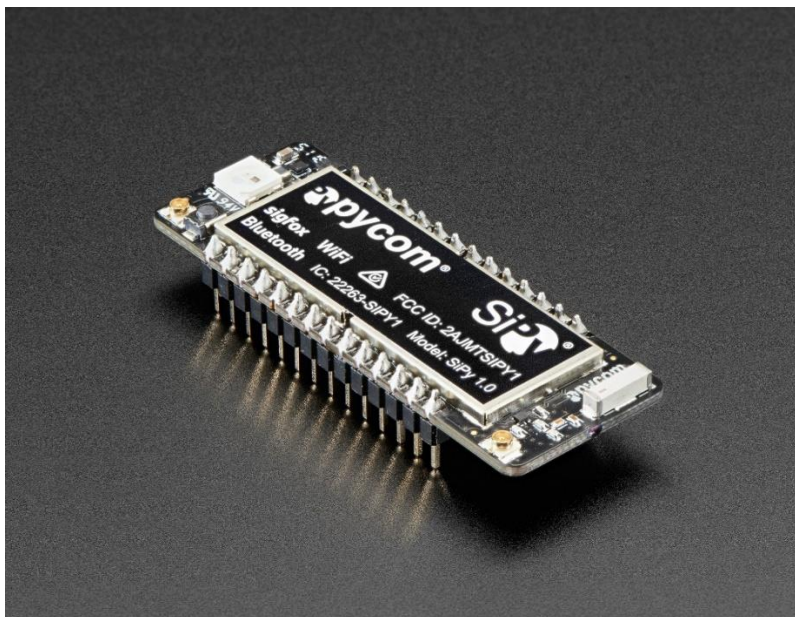
Kartoitan työssä erilaisten protokollien nykyhetken käyttötarkoitusta ja tulevaisuuskuva. Tavoitteena on saada yleiskuva eri tarkoituksiin soveltuvista IoT:n protokollista, jolloin tuotetta suunniteltaessa voidaan tehdä oikeita valintoja, kun halutaan keskittyä esimerkiksi tietoturvaan. Vaikuttavia tekijöitä on protokollan tietoturvan nykytilanne, haasteet, tulevaisuusnäkökulma, sekä tekninen suorituskyky esimerkiksi yhteyden kantaman tai tiedonsiirtokyvyn kannalta. Kiinnitän erityisesti huomiota DigiOS-projektin käytössä oleviin protokollisiin.

DigiOS-projektiin liittyen teen katsauksen myös heidän tietoturvaan keskittyvään malliin. Siinä alueena on laitteen yhteysprotokollan lisäksi käytettävät laitteet, kuten Bittium Tough Mobile, MySQL- ja NoSQL-tietokantapalvelimet sekä näiden väliset yhteydet. Tavoitteena on saada kuva tietoturvan tilasta. Tähän työhön ei liity käytännön tehtävää, vaan se toteutetaan tutkimustyönä.

2. IoT:n kasvu ja tietoturva

Internet of Things on vielä yli kymmenen vuoden kehittymisen jälkeenkin kasvava teknologian alue. Vasta viime vuosina on päästy verkon ja laitteiden puolesta sellaiselle tasolle, että byrokrattisemmatkin alat ovat saaneet aloitettua projekteja IoT:n käyttöönottamiseksi. Laitteita otetaan käyttöön kasvavalla tahdilla. Cisco arvioi vuonna 2014, että vuoteen 2020 mennessä päästäisiin 50 miljardiin laitteeseen, mutta se on osoittautumassa optimistiseksi, sillä nykyisten arvioiden mukaan laitemäärä on nousemassa noin 30 miljardiin vuoteen 2020 mennessä. [1.]

Teollisuudessa IoT luo pienlaitteilla ja sensoreilla uusia mahdollisuuksia monitorointiin. Tuotannon eri vaiheista saadaan entistä paremmin dataa, jolloin sen tilaa voidaan tarkkailla tehokkaammin. Tämä tuo myös ongelmakohtat paremmin esille, jolloin niihin reagoiminen on tehokkaampaa. Tehokkuuden kasvaessa suhteelliset kulut laskevat. Nopeammin huomattavat ongelmakohtat ja pullonkaulat tuovat yrityksille säästöjä paikoista, joista aikaisemmin vähäisemmällä monitoroinnilla ei olisi mitään edes löytynyt. Eräitä merkittävimmistä IoT:n tuomista monitoroinnin edistyksistä ovat laitteiden pieni koko, vähäinen virrankäyttö, sekä langattomat yhteydet. Pienet laitteet saadaan mahdutettua helposti ahtaisiin tiloihin, eikä laitteisiin yhteyden saamisesta tule päänvaivaa monipuolisten langattomien yhteysprotokollien ansiosta. Pienissä mikrokontrollereissa voidaan käyttää enemmänkin, kuin yhtä teknologiaa kerralla uhraamatta laitteen kokoa.



Kuva 1. Pieni SiPy-mikrokontrolleri, jossa on vastaanottimet Sigfoxille, WiFille ja Bluetoothille.

Lähde: Adafruit Industries, Flickr, 2017. [2.]

Terveydenhuollossa on yhtäläisyyksiä teollisuuden kanssa, mutta päätavoitteena vaikuttaa olevan potilaan arjen helpottaminen. Käyttöön halutaan ottaa pieniä puettavia ja iholle kiinnitettäviä laitteita, joilla potilaiden tilaa voidaan seurata myös heidän kotonaan. Näin potilaita pystytään lähettämään aikaisemmin kotioloihin, eikä sairaalakustannuksia pääse syntymään niin paljon. Myös potilas hyötyy tästä, sillä sairaalassa vietettävä aika vähenee nykyisestä, jolloin arkielämään palaaminen on nopeampaa. Myös joitain pitkäaikaisempia sairauksia pystyttäisiin tarkkailemaan potilaan kotona ilman jatkuvia sairaalakäyntejä. Tämä vapauttaa sairaalan työntekijöiden työtaakkaa sekä nopeuttaa hoitoon pääsemistä muille potilaille.

Kotitalouksissa IoT:n tuomat hyödyt ovat pieniä elämää helpottavia asioita. Yksinkertaisia asioita, kuten valojen, laitteiden ja lämmön säätämistä, sekä palohälytyksistä ilmoittamista puhelimeen pystytään jo tekemään IoT-laitteilla. Pienillä laitteilla pystytään keräämään tietoa ihmisten elämästä ja esittämään tätä tietoa siten, että sen perusteella pystytään tekemään muutoksia. Tulevaisuudessa esimerkiksi jääkappeihin voidaan saada älyä ostosten seuraamisen muodossa. Tällä hetkellä IoT:n tuomat edut kotitalouksissa eivät ole yltäneet köyhiin talouksiin, sillä se on vielä suurelta osalta luksusta, eikä oikeasti tarpeellista. Tulevaisuudessa hinnat saattavat kuitenkin laskea ja käyttötarkoitukset kehittyä, jolloin IoT-laitteiden käyttö voi yleistyä.

Esineiden internetin tietoturva on noussut keskustelun aiheeksi sen kasvaneen suosion mukana. Ensimmäisenä markkinoille tulleet laitteet toteutettiin yleisesti toiminnallisuus ensin -periaatteella. Tämä tarkoittaa sitä, että esimerkiksi tietoturvaan ei kiinnitetty paljoa huomiota, vaan laite tehtiin nopeasti toimivaksi ratkaisuksi ja työnnettiin markkinoille. Tällaisen käyttäytymisen muuttaminen on aikaa vievä prosessi, sillä hataralla turvallisuuspohjalla olevia laitteita ei välttämättä voi päivittää kunnolla, tai niissä tehdyt ratkaisut ovat pohjimmiltaan niin väärin, ettei asiaa voi korvata muuten kuin alusta aloittamalla. Laitteiden hinnasta on myös tingitty, massatuotannon helpottamiseksi. Tietoturvan huomiointi vaatii usein erillisiä tai tietoturvaa varta vasten tehtyjä komponentteja, eivätkä ne ole ilmaisia.

Esineiden internetin laitteet ovat monesti pienikokoisia. Tämä asettaa tiettyjä rajoitteita käytössä olevilla komponenteilla ja samalla nostaa erikoistuneempien komponenttien hintaa, jos laatu halutaan taata. Laitteet on monesti koonsa ja lukumääränsä vuoksi sijoitettu paikkoihin, joita ei pystytä turvaamaan. Tietoturvan saralla pitää siis huomioida, että ulkopuoliset henkilöt voivat päästä käsiksi laitteisiin tilanteesta riippuen helpommin kuin esimerkiksi turvallisessa konesalissa olevaan palvelimeen.

3. IoT-järjestelmät

Internet of Thingsissa pääpiirteensä on tiedon tai datan kerääminen paikoista ja asioista, joita ei ennen pystytty tehokkaasti mittamaan. IoT:iin kuuluvia järjestelmiä on lukuisia, eikä niistä ole helppoa eritellä muita yhteisiä määrittäviä tekijöitä kuin pieni dataa keräävä anturi. Näitä antureita voi järjestelmissä olla käytettävistä teknologiasta riippuen miten monta vain. Dataa keräävän anturin lisäksi tässä työssä merkittävänä tekijänä on IoT-järjestelmän yhteydet sekä datan vastaanottaja.

Suunnitteluvaiheessa tulee määrittellä laitteen vaatimukset, kuten tarvittavat datamäärät ja tietoturva, sekä virrankäytön huomioon otavat asiat. Vaatimuksia voi olla muitakin, mutta vasta vaatimusten määrittämisen jälkeen voidaan kunnolla tehdä päätöksiä sopivista ja sopimattomista laitteista. Vaatimuksia vastaava järjestelmä voi löytyä valmiina pakettina, mutta käyttötapauksien kirjon vuoksi on myös mahdollista, ettei sopivaa toteutusta löydy valmiina, jolloin se täytyy tehdä joko ulkopuolisen tahon kautta tai rakentaa itse. [3.]

3.1 IoT-laite

Internet of Thingsissa käytettäviä antureita ja laitteita on monenlaisia. Näillä mittalaitteilla on usein yksi tai muutama asia, joita ne mittaavat, mutta yleisesti ne ovat erikoistuneita yksittäisiin asioihin. Mitattavia asioita voi olla kaikki ilmankosteudesta lämpötilaan, henkilön pulssista sijaintitietoihin, tai vaikka postipakettien saapuminen. Melkein kaikkea varten pystytään tekemään Internet of Thingsin alueella dataa keräävä anturi.

Laitteet ovat usein pieniä ja vähävirtaisia, minkä vuoksi niiden sijoittaminen on helppoa. Monet IoT-tekniikat mainostavat erityisesti vähävirtaisuudellaan, sillä antureista halutaan pitkäikäisiä, eikä virtalähteeksi välttämättä saada mitään nappiparistoa ihmeellisempää toteutusta. Tästä huolimatta joidenkin laitteiden toimintaiäksi luvataan jopa vuosia yksittäisellä paristolla. Pieni koko voi myös olla tärkeä mahdollistaja, sillä IoT-laitteille ei tarvitse varata paljoa tilaa. Kuluttajillekin on myynnissä luottokortin kokoisia Raspberry Pi -pienetietokoneita, joita voidaan hyödyntää anturin kanssa IoT-järjestelmässä. Laitteita on paljon, eikä valinta ole helppoa. Valmiita ratkaisuja on olemassa, mutta käyttötarkoitukseen sopivan löytäminen voi viedä huomattavasti aikaa. Jos tavoitteena on laajempi tuotteen levittäminen, voi kokonaan oman toteutuksen kehittäminenkin

olla kannattavaa, sillä valmiista ratkaisuista voi olla hankalaa löytää juuri omaan käyttötarkoitukseen sopivaa laitetta.

3.2 Yhteydet

Laitetta valittaessa tulee vastaan myös kysymys, minkälaista yhteyttä järjestelmä tarvitsee tai vaatii. On olemassa lukuisia protokollia, jotka keskittyvät yksittäiseen ominaisuuteen, kuten esimerkiksi helppokäyttöisyyteen Bluetooth, signaalin kantomatkaan Sigfox tai energiatehokkuuteen. Laitteen käyttötarkoitus usein määrää protokollat, joita siinä voidaan käyttää. Tämän jälkeen tulee enää eteen tietyn teknologian toteuttamisen hinta. Avoimeen lähdekoodiin perustuvat toteutukset ovat monesti helpommin muokattavissa käyttötarpeisiin, mutta esimerkiksi pitkäaikainen tuki laitteille on vaikeaa toteuttaa tästä syystä. Suljetummat teknologiat ja valmiit kokonaisuudet taas tuovat mukanaan hyvää tukea ja toimivan paketin, mutta erityisiin käyttötarkoituksiin mukautuminen voi olla hankalaa korkeampien hintojen vuoksi.

Jos yhteyksistä haluaa tietoturvallisia, ovat valmiit paketit yleensä parhaita ratkaisuja projektin toteuttamiseen, sillä yleensä tietoturvan vaatimukset ovat tarkkoja, eikä niitä ole helppo toteuttaa ilman kyseisen teknologian asiantuntijoita. Monet langattomat protokollat eivät ota kantaa yhteyden tietoturvallisuuteen kovin syvällisesti, tai pesevät kätensä kokonaan asiasta. Onneksi kuitenkin on jo kehitetty tietoturvaan keskittyviä protokollia, kuten Z-Wave ja jossain määrin Sigfox, sekä parannettu vanhoista protokollista uusiin versioihin, kuten 2G, 3G ja 4G -mobiiliverkoissa. Näin tietoturvaa vaativille toteutuksillekin ollaan saatu enemmän vaihtoehtoja pelkkien omien ratkaisuiden lisäksi.

3.3 Vastaanottaja

Kun käytettävä yhteys on valittu, täytyy vielä suunnitella ja toteuttaa yhteyden vastaanottava pää. Koska tietoturvan puolella koko järjestelmä on yhtä vahva, kuin sen heikoin lenkki, on järjestelmän jokainen kohta arvioitava ja tarvittaessa turvattava. Sensorilta lähtevän datan vastaanottajalta datan siirtäminen palvelimelle ja palvelimella olevan datan turvaaminen ovat myös osana koko järjestelmän tietoturvaa. Useimmiten, jos tarvitaan erityisen tietoturvallista ratkaisua verkon yli datan siirtoon, toteutetaan yhteys VPN:llä, eli virtuaalisella erillisverkolla. Yhteys voidaan toteuttaa fyysisesti erillisenä yhteytenä, tai yleisen internetin yli kulkevana salattuna yhteytenä.

Fyysisesti erillinen yhteys on kauttaaltaan turvallisempi, mutta usein myös kalliimpi toteuttaa, sillä laitemäärien ja etäisyyksien kasvaessa sopivan toteutuksen löytäminen tai tekeminen vaatii yhä enemmän varta vasten varattua infrastruktuuria. Esimerkiksi erillisen verkkoyhteyden tekeminen konesalien väliin voi maksaa helposti satoja tuhansia euroja.

Yleisen internetin yli kulkevan salatun yhteyden toteuttaminen on tästä syystä varteenotettava vaihtoehto, vaikka se on vähemmän tietoturvallinen. Yhteys tulee salata, ettei salakuunteleminen onnistu, ja yhteyden vastaanottava ja lähettävä pää turvata tarpeeksi hyvin kustannukset ja riski huomioon ottaen. Ulkopuolisten ei pitäisi päästä käsiksi tietoihin katsomaan niitä, muokkaamaan niitä, eikä estämään niiden kulkua. Kaikkiin järjestelmiin ei kuitenkaan tarvitse saada sotilastason tietoturva, sillä turvattava tieto ei välttämättä ole turvaamisen kustannuksien veroista. Riskit pitää silti tunnistaa ja hyväksyä, jotta pystytään tekemään toimiva ohjeistus häiriötilanteita varten tietoturvan osalta.

3.4 Standardisoinnin tarve

Erilaisia järjestelmiä ja laitteita on paljon. Jokainen niistä vaikuttaa omalla tavallaan järjestelmän yleiseen tietoturvaan, ja määrittää tehtäviä asioita tietoturvan takaamiseksi. Läheskään kaikki teknologiat eivät toimi toistensa kanssa, ja oikeastaan yhteensopivuus täytyy tutkia tapauskohtaisesti asiantuntijoiden kanssa. Tämän takia valmiit ratkaisut on usein kustannustehokkain vaihtoehto, sillä joku muu on jo tehnyt ajatus- ja kehitystyön tietoturvallisen järjestelmän tai toimintamallin aikaan saamiseksi.

IoT:sta puuttuu kattavammat standardit, jotka auttaisivat yhteensopivuuden kanssa. Toki on olemassa esimerkiksi matkapuhelinverkkojen standardit, jotka ovat samankaltaisia ympäri maailman, mutta vähävirtaisia langattomia protokollia on yleisesti lukuisia, ja ne toimivat monesti täysin omilla alustoillaan. Isommat yritykset yrittävät kuitenkin saada omia standardejaan laajempaan käyttöön, mutta sen onnistuminen on aina kiinni siitä, saavatko he tarpeeksi kattavaa tarjontaa aikaan järkevästi. Tällaisia tapauksia on esimerkiksi Bluetooth Special Interest Groupilla, SIG:illä, heidän Bluetooth Low Energy -protokollan kanssa, sekä Googlen takaamalla Thread-protokollalla, unohtamatta 3GPP:n sekavahkoa LTE-IoT protokollakasaa. Yksittäistä voittajaa ei näistä ole vielä löytynyt, eikä IoT:n erittäin laajan vaatimuskirjon vuoksi välttämättä löydykään pitkään aikaan.

4. Yhteysprotokollat ja standardit

Laitteiden suuren määrän lisäksi erilaisten protokollien määrä vaikeuttaa huomattavasti päätöksentekoa, kun pohditaan, olisiko järkevää kehittää uusi laite vanhojen käyttämisen sijaan. Uusia, entistä parempia teknologioita kehitetään koko ajan, eikä eri teknologioiden ominaisuuksista ota helposti selkoa ilman asiantuntijoiden apua. Tässä kappaleessa esittelen tunnetuimpia teknologioita, niiden käyttötarkoituksia, ominaisuuksia, sekä selvitän myös tietoturvan kannalta teknologian kannattavuutta. Esiteltyt asiat on kuvattu tiivistäen ja tyypillisimpiä ominaisuuksia tarkastellen.

4.1 WiFi

WiFi on langaton lähiverkkoprotokolla, joka on laajassa käytössä esimerkiksi tietokoneissa ja matkapuhelimissa. Alun perin se kehitettiin langattomaksi vastineeksi Ethernet yhteydelle ja se on yleisesti tunnettu helposta käyttöönotosta ja halvasta hinnasta, mutta IoT:n alalle WiFi:n virrankäyttö ei ole halutulla tasolla. Keskivertaisen kantaman lisäksi verrattain korkea virrankäyttö estää WiFi:n laaja-alaisen käytön IoT-laitteissa. Tästä syystä tekeillä on uusia standardeja, joiden avulla parantavan WiFi:n energiatehokkuutta sekä verkon tehokkuutta ja kantamaa. Normaali WiFi käyttää useimmiten joko 2,4 GHz tai 5,8 GHz radiotaajuutta. Nämä taajuusalueet on käytössä jaettu pienempiin osiin liikennemäärän tuoman kuorman vuoksi, sillä WiFi:n lisäksi esimerkiksi 2,4 GHz radiotaajuutta käyttää myös Bluetooth ja mikroaaltouunit. Tarkat taajuusalueet vaihtelevat alueen mukaan, sillä eri maissa käytössä voi olla eri taajuudet. [3.]

Vuonna 2016 julkaistiin IEEE 802.11ah, toiselta nimeltään WiFi HaLow, joka otti käyttöön 900 MHz kaistan. Näin virrankäyttöä saadaan alennettua, jolloin myös tuettu laitemäärä nousee, tukien samalla IoT:n vaatimuksia. WiFi HaLowin käyttöönottoa hidastaa hieman eri maiden 900 MHz:n taajuuden käyttö, sillä eri maissa taajuuksia käytetään eri tarkoituksiin, eikä 900 MHz taajuus ole kaikkialla saatavilla. Markkinoilla ei vielä ole WiFi HaLowia käyttäviä laitteita, mutta ne ovat kehitteillä. Katseet ovat myös 2019 julkaistavassa WiFi 6 -standardissa, aikaisemmalta nimeltään 802.11ax, jonka arvioidaan parantavan merkittävästi datan siirtonopeutta ja vähentävän yhteyksien ruuhkautumista ja virran kulutusta. [4.] [5.]

WiFi ei ole kovin tietoturallinen standardi. Kuka tahansa pystyy yrittämään verkkoon kirjautumista, jos vain huomaa verkon olevan olemassa. Verkon SSID:n, eli esimerkiksi tietokoneella näkyvän verkon nimen voi piilottaa, mutta verkkoskannerilla verkon pystyy silti löytämään ja siihen kirjautumista yrittämään. WiFi-verkon tietoturvan kanssa tuleekin olla erityisen huolellinen, sillä oletussalasanat saadaan helposti selville ja reitittimien asetusten heikkouksia on suhteellisen helppo käyttää hyväksi. Useimpien laitteiden tehdasasetteiset salasanat ovat löydettävissä Internetistä, eikä päättävälle murtautujalle yksinkertaiset salasanatkaan ole ongelma. Laitetta käyttönotettaessa täytyy huomioida käytettävää salaus, sekä muut langattoman tukiaseman asetukset, sillä lähtökohtaisesti vastuussa on laitteen käyttäjä.

4.2 Bluetooth ja BLE

Yleisesti matkapuhelimeissa ja niiden oheislaitteissa käytössä oleva Bluetooth on sen korkean käyttöasteen ja yhteensopivuuden vuoksi helppo vaihtoehto IoT-laitteen yhteyden toteutukseen. Klassista Bluetoothia käytetään yksittäisten laitteiden toisiinsa yhdistämiseen hieman WiFiä pienemmällä alueella. Sen käyttötarkoituksia on esimerkiksi langattomien hiirien yhdistäminen tietokoneisiin tai kuulokkeiden liittäminen älypuhelimeen. Matkapuhelinten rajattu akun kesto on ajanut Bluetoothin parantamaan energiatehokkuuttaan, sillä etenkin vanhemmat Bluetoothin versiot tyhjänsivät matkapuhelinten akkuja tehokkaasti, jos Bluetooth jätettiin vahingossa päälle. Bluetoothin helppokäyttöisyys ja levinneisyys sekä energiatehokkuuden parannukset ovat kuitenkin saaneet sen jäämään laajaan käyttöön, sillä kaikki nykyiset matkapuhelimet tukevat Bluetoothia. Levinneisyys ja helppo käyttöönotto houkuttelivat Bluetoothin käyttämiseen myös Internet of Thingsin alalla. Huomattiin nopeasti, että IoT-laitteiden erittäin rajattu virransaanti on suuri haaste Bluetoothin kanssa. Haluttiin myös tukea isommalle määrälle laitteita samaan aikaan, kuin mitä klassiset Bluetoothin versiot tukivat.

Bluetooth Low Energy, eli BLE, on Bluetoothin IoT:ta varten kehitetty versio, jossa vähäiseen virrankulutukseen on keskitytty paljon. Se sopii erityisen hyvin laitteille, joiden halutaan toimivan pitkään pienellä virtalähteellä, kuten kolikkopatterilla. Huonona puolena on suurempien tiedostojen siirtäminen, sillä yhteyden kapasiteetti on melko pieni, noin megabitti sekunnissa. Osittain tätä helpottaa, että suuri osa BLE:n kanssa yhteensopivista laitteista on myös normaalin Bluetoothin kanssa yhteensopivia, joten suurempien datamäärien siirron, kuten esimerkiksi päivitysten tekemisen voi tehdä normaalilla Bluetoothilla, mutta laitteen perustoiminta käyttää silti BLE:ä.

Vähäinen virrankulutus ei myöskään haittaa BLE:n kantamaa, sillä kantama on arviolta 50 metristä 150 metriin alueesta riippuen. [1.]

Bluetoothin suurin tietoturvaongelma on laitteiden yhdistämisvaiheessa. Helpoimmin toteutetut yhdistämistavat on myös helpoimpia salakuunnella tai muuten murtaa, mutta turvallisemmat vaihtoehdot joko nostavat tai vaikeuttavat käyttäjäkokemusta. Esimerkiksi Out-Of-Band -yhdistäminen on tietoturvallinen hyvin toteutettuna, mutta se vaatii laitteiden yhdistämisen jotain muuta protokollaa tai reittiä pitkin, kuin itse Bluetoothin. Tämä voidaan toteuttaa esimerkiksi toisella langattomalla protokollalla, kuten NFC-sirulla, mutta toteutuksen hinta nousee lisättävästä protokollasta riippuen, joten tilanne täytyy arvioida tapauskohtaisesti. Helppokäyttöinen Just Works™ -yhdistäminen tapahtuu laitteiden välillä automaattisesti. Ainoastaan Bluetooth 4.2 versiossa tätä yhdistämistä voi ajatella jossain määrin turvallisesti, mutta koska käyttäjä ei pysty varmentamaan yhdistettyjä laitteita mitenkään, voidaan yhteys kaapata ja salakuunnella ilman käyttäjän tietoisuutta. [6.]

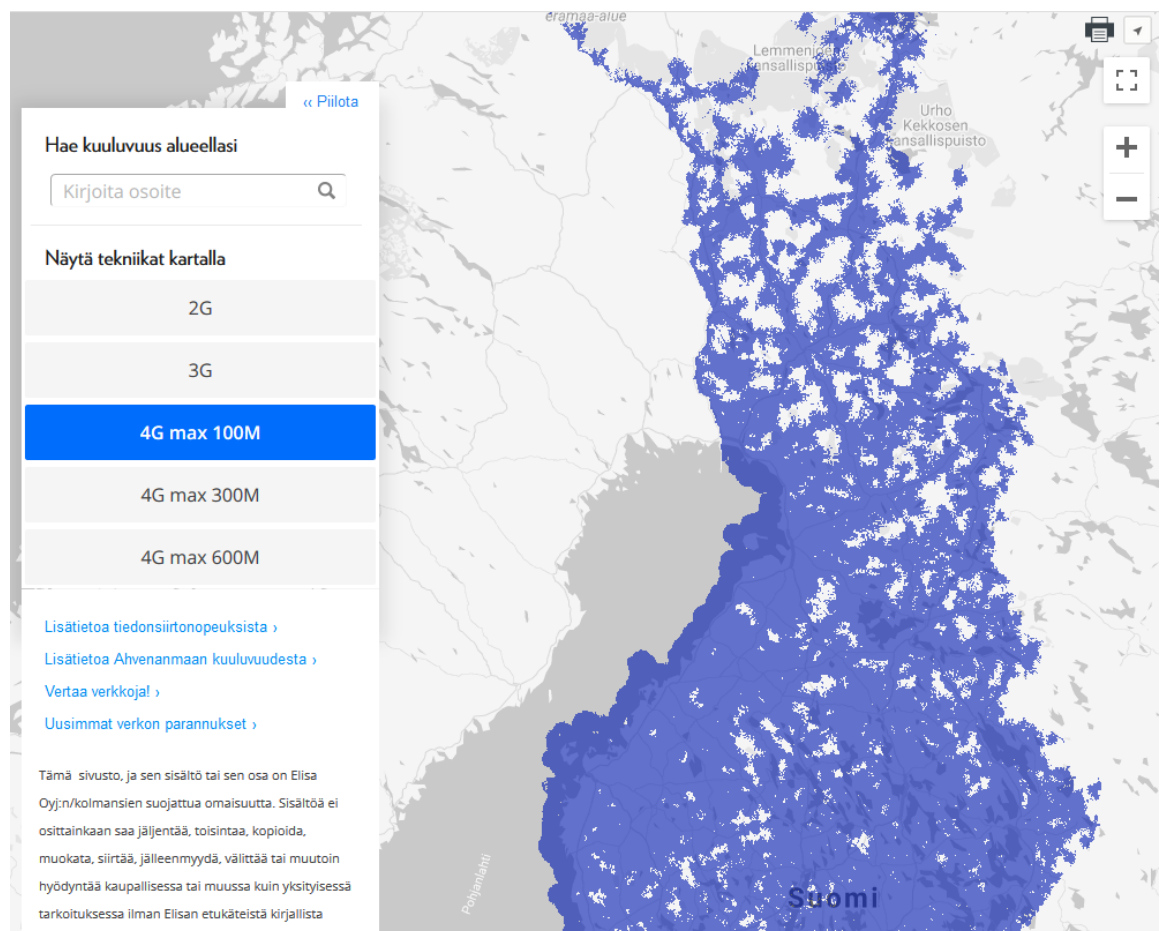
4.3 Matkapuhelinverkko

Matkapuhelimissa on jo vuosia ollut käytössä Bluetoothin lisäksi energiatehokas verkkototeutus, jonka sopivuus IoT:n vaatimuksiin huomattiin nopeasti. 2G, 3G, 4G ja tulevaisuudessa 5G ovat matkapuhelimille suunnattuja telekommunikaatioteknologioita, joiden energiatehokkuuden ja katealueen ansioista niitä on otettu käyttöön myös matkapuhelinten ulkopuolella. Niiden käyttöönotto on verrattain helppoa, sillä niitä käyttävät laitteet ovat yleisesti käytössä ja niiden vaatima infrastruktuuri on rakennettu jo aikaisemmin.

Näiden verkkoteknologioiden suorituskyky ja luotettavuus on parantunut sukupolvien välillä pienempien parannuksien myötä. Sukupolvet ovat toisistaan erillisiä käytössä olevaa rautaa myöten. Siksi käytettävää teknologiaa valittaessa on tärkeää huomioida teknisten vaatimusten lisäksi, että uudempien matkapuhelinverkkojen vaatima rauta on usein kalliimpaa, kuin vanhemmilla sukupolvilla. Tietenkin hinta tuo mukanaan myös merkittäviä parannuksia suorituskykyyn, energiatehokkuuteen, sekä luotettavuuteen, mutta aina ne eivät ole hinnanlisäyksen arvoisia ominaisuuksia. Vanhempia sukupolvia arvioidessa täytyy myös ottaa huomioon käyttöikä; IoT-laitteet on usein tarkoitettu kestämään vuosia, ellei vuosikymmeniä. Täytyy pohtia, kannattaako näin pitkäikäisen laitteen verkko toteuttaa esimerkiksi 2G-teknologialla, kun sitä on jo alettu poistamaan käytöstä joissain maissa. [7.]

4.3.1 4G LTE

3GPP Long Term Evolution, on langattoman verkon teknologia, josta monesti puhutaan 4G LTE:nä. Se perustuu 3GPP:n, eli 3rd Generation Partnership Projectin, kehittämään LTE -standardiin, mutta LTE-standardin vaatimukset datan siirrossa ovat huomattavasti korkeammalla, kuin 4G LTE:n nopeudet. 4G LTE ylittää 100 megabitin latausnopeuksiin ja 50 megabitin lähetysnopeuksiin, mutta LTE-standardin vaatimuksena on 1000 megabitin lataus- ja 500 megabitin lähetysnopeudet. Tästä huolimatta 4G LTE on levinnyt matkapuhelinkäytössä maailmanlaajuisesti teknologiksi ja sitä käyttävät tällä hetkellä kaikki suurimmat teleoperaattorit, joskin hieman eri taajuuksilla riippuen maantieteellisestä sijainnista. Esineiden internetin käyttötarkoituksiin 4G sopii matkapuhelinten tyyppisiin laitteisiin, jotka tarvitsevat langatonta yhteyttä pienessä paketissa laajalla alueella. Sen käyttöönoton etuna on jo valmiina oleva 4G-infrastruktuuri, jolla on hyvä katealue alueesta hieman riippuen. [6.]



Kuva 2. Elisan 4G-verkon kuuluvuudessa on aukkoja hajanasemmin asutetuilla paikoilla enemmän mitä pohjoisemmaksi Suomessa liikutaan. Muidenkin operaattoreiden tarjonta on samankaltainen. Lähde: Elisa Kuuluvuuskartta. [7.]

Esineiden internetiä varten on myös kehitetty oma versio 4G LTE:stä, Narrowband IoT, tai NB-IoT. Sen etu normaaliin 4G LTE:hen verrattuna on suurempi laitemäärä, vähäisempi virrankulutus, sekä parempi katealue. NB-IoT ei toimi aivan yhtä nopeasti, kuin 4G LTE, sillä sen siirtonopeus on enintään 250 kilobittiä sekunnissa, mutta esineiden internetin pienien datamäärien takia tämä ei usein ole ongelma.

4G LTE:n turvallisuus voi helposti olla huolen aiheena, sillä sen käyttö on levinnyt niin laajalle, että sen murtaminen on varmasti joillakin tahoilla tavoitteena. Ars Technican Sean Gallagher pohti artikkelissaan, että 4G LTE:n turvallisuus perustuisi pohjimmiltaan epämääräisyyteen. Eri alueiden verkkototeutuksissa on sen verran eroja, jolloin yhdessä paikassa toimiva haavoittuvuus ei välttämättä toimi muualla. Tämän lisäksi mobiiliverkkojen toteutukset on piilotettu verhojen taakse, eikä niistä ole saatavilla kattavasti yleistä tietoa. [8.]

4.3.2 3G ja 2G

2G ja 3G -yhteydet, eli toisen ja kolmannen sukupolven matkapuhelinteknologiat, ovat vielä käytössä, vaikka 4G on otettu laajasti käyttöön, ja 5G on parhaillaan kehitteillä. Niiden etuna uudempiin teknologioihin on parempi katealue, sillä mailla ja operaattoreilla on ollut vuosia aikaa rakentaa niitä varten infrastruktuuria. Tästä huolimatta niiden käyttöönottamista IoT-ratkaisuissa tulee harkita, sillä ajan myötä vanhemmat teknologiat tullaan poistamaan käytöstä. Näin on käynyt jo esimerkiksi USA:ssa, jossa yksi suurimmista teleoperaattoreista AT&T lopetti tuen 2G langattomille verkoille vuonna 2017. Käytettävää yhteyttä valittaessa tuleekin huomioida laitteen pitkäikäisyys. Uudemmissa teknologioilla voi kalliimman hinnan kanssa tulla myös etuja, kuten parannettu energiatehokkuus ja siirtonopeus tai datan katkeamattomuus siirryttäessä alueelta toiselle.

Nopeuden puolesta jokainen sukupolvi on edeltäjäänsä nopeampi. 2G voi siirtää 256 kilobittiä sekunnissa. 3G paransi siitä 120-kertaiseksi 30 megabittiin sekunnissa. 4G nosti datamäärän 200 megabitin tienoille ja tulevan 5G:n odotetaan parantavan yli gigabittiin sekunnissa. Korkeammat nopeudet tarkoittavat myös, että nopeutta rajoitettaessa esimerkiksi IoT:n pienlaitteelle, virrankulutus laskee verrattuna täyteen verkon nopeuteen. 4G/LTE:n etuna on myös varayhteys 2G- ja 3G-verkkoihin, jos yhteys 4G:n mastoon katkeaa. Jos yhteyttä ei käytetä paljoa, eikä dataa lähetetä suuria määriä, ja jos muut vaatimukset täyttyvät vanhemmilla teknologioilla, on 2G ja 3G rahallisesti kannattavampia vaihtoehtoja 4G:hen verrattuna. [6.]

4.4 ZigBee

ZigBee on avoimen lähdekoodin teknologia, jota käytetään vähävirtaisissa, sulautetuissa laitteissa tehokkaan laitteiden välisen kommunikaation vuoksi. ZigBeen kantomatka on paikasta riippuen 10-100 metriä, mutta pidemmät kantamat vaativat enemmän virtaa. MIT:n tutkijoiden tekemän tietoturvaselvityksen mukaan ZigBee on pohjimmiltaan tietoturvallinen, mutta avoimen lähdekoodin tuoman vapauden vuoksi sitä käyttäville tuotevalmistajille jää vastuu protokollan ohjeiden ja hyvien käytänteiden noudattamisesta. Oman käyttötarkoituksen vaatimukset tulee olla tiedossa, ja vaatimusten täytyminen tulee tarkistaa tuotevalmistajalta. Zigbee ei yllä aivan samoihin siirtonopeuksiin, kuin BLE, mutta se tukee huomattavasti enemmän samanaikaisia laitteita pitäen virrankulutuksen siitä huolimatta verrattain matalana. [4.] [9.]

Merkittävin tietoturvaohue on laitteiden liittämisvaiheessa, sillä ZigBee on ottanut tietoisien riskien yhteensopivuuden ja tehokkuuden takaamiseksi. ZigBee olettaa, että tunnistusvaiheita vaihtaessa, eli laitteiden liittyessä toisiin, laitteet olisivat tietoturvallisia, mutta tästä syystä on mahdollista liittyä ZigBee-verkkoon jäljittelemällä luotetun laitteen yhdistämisvaiheessa lähettämiä verkkopaketteja. Tämän haavoittuvuuden voi kiertää käyttämällä jotain toista tapaa tunnistaa yhdistettävä laite, kuin käyttämällä samaa ZigBee verkkoa. Vaihtoehtoisia tunnistautumistapoja on esimerkiksi erillinen langallinen yhteys, NFC-yhteys, eli parin senttimetrin etäisyydeltä toimiva Near Field Connection, tai jokin muu tapa jakaa tunnistusavain laitteiden välillä. Toisaalta tällaiset erilliset Out-of-Band toiminnot tuovat laitevalmistajille lisäkustannuksia. [10.]

4.5 Z-Wave

Z-Wave on tanskalaisen Zensysin kehittämä verkkoprotokolla, joka toimii 908 MHz:n taajuudella USA:ssa, ja vaihtelevasti muita taajuuksia riippuen maasta. Vaikka maakohtainen taajuus tuokin ongelmia, on 900 MHz:n taajuusalue sen verran vähemmän käytetty, kuin esimerkiksi 2,4 GHz:n taajuus, että yhteydessä on huomattavasti vähemmän taustamelua ja parempi kuuluvuus. Siinä kuitenkin vallitsee alueelliset erot samalla lailla, kuin WiFi HaLow:ssa, sillä kaikkialla tämä taajuusalue ei ole yleisessä käytössä. [11.]

Z-Wavea on markkinoitu laajasti tietoturvallisena protokollana. Tietoturvaan keskittyminen tuo Z-Wavea käyttävien tuotteiden hintoja hieman ylös, mutta Z-Waveen kohdistuvia hyökkäyksiä ei

ole paljoo, etenkin jos puhutaan Z-Waven S2-tietoturvapäivityksestä. Kaikki Z-Wavea käyttävät laitteet eivät tue S2-tietoturvastandardin, mutta Z-Waven verkkosivuilla on kattava lista laitteista, jotka käyttävät Z-Wavea ja tukevatko ne uutta tietoturvastandardia. Laitetta valitessa täytyy kuitenkin olla tarkkana, sillä Z-Wave-protokollaa käytettäessä valmistajalla on viime kädessä vastuu sen hyvien käytänteiden mukaisesta soveltamisesta. Hyvin tehtynä laite saa jatkuvasti tietoturva- ja ohjelmistopäivityksiä, mutta huonosti tehtynä erilaisia ohjelmistovikoja ei välttämättä korjata ajoissa, eikä päivityksiä tietoturvaohjelmille välttämättä tule ollenkaan. [12.]

4.6 Sigfox

Sigfox-tekniikka on samalla nimellä kulkevan yrityksen kehittämä mobiiliverkkoa muistuttava tekniikka. Sigfox operoi itse tukiasemiaan, joten sen voisi rinnastaa puhelinverkkojen palveluntarjoajiin. Toisin kuin mobiiliverkot, Sigfox on suunniteltu pieniä yksittäisiä datamääriä varten. Yksi verkon objekti voi lähettää maksimissaan 140 viestiä päivässä. Viestin maksimikoko on 12 tavua ja tiedonsiirtonopeus on noin 100 bittiä sekunnissa. Kyseessä on siis erittäin pieniä datamääriä, joita ei tarvitse lähettää kovin montaa kertaa päivässä. Se myös toimii hyvin kapealla kaistalla, minkä ansiosta sen radiolähetimet eivät kuluta paljoo virtaa. Sigfoxin pienet datamäärät ja virrankulutus sopii hyvin esimerkiksi GPS-järjestelmiin, sillä vähävirtaisuudesta huolimatta Sigfoxin kantama on merkittävä. Keskimäärin signaali kantaa 30-50 kilometriä harvaan asutetuilla alueilla, ja 3-10 kilometriä kaupungeissa. Pisin mitattu kantama Sigfoxilla on 1258 kilometriä. Mittaus tehtiin avomeren yli Portugalista Kanarian saarille. [13.] [14.] [15.]

Sigfoxin tietoturvasta ei ole kovin paljon tutkimuksia saatavilla, mutta esimerkiksi WND Groupin mielestä Sigfox on erittäin tietoturvallinen tekniikka. He perustelevat tätä sillä, että Sigfox ei käytä TCP/IP -protokollaa, jolloin laitteisiin ei pääse suoraan internetistä kiinni. Tämän lisäksi Sigfoxin käyttämä palomuri on erittäin tiukka. Laitteet toimivat pääasiassa yhteydettöminä, mutta kun tarve datan lähettämiseksi syntyy, laite lähettää tukiasemille radioviestin, joka kulkee Sigfox Core Networkiin. Core Networkista se siirretään relevanttiin IoT-järjestelmään. [16.]

Jokaisessa Sigfox-laitteessa on erillinen muisti, johon on talletettu uniikki avain. Tähän muistiin ei voi kirjoittaa mitään, joten avainta ei pysty muuttamaan. Tätä avainta käytetään viesteissä lähetettävän laitteen todentamiseen. Yhteyttä ottaessaan Sigfoxin päätelaite lähettää radioviestin moneksi tukiasemalle kolmeen kertaan valitsemalla jokaiselle viestille oman satunnaisen taajuuden

Sigfoxin taajuusalueesta. Näin viestien kaappaaminen tai muuttaminen matkan varrelta on erittäin vaikeaa.

Sigfox vaikuttaa luotettavalta teknologialta tietoturvatoteutuksensa puolesta. Teknologiaa käyttävälle taholle jää kuitenkin vastuu oman osansa järjestelmästä turvaaminen. Sigfoxia harkitessa pitää myös miettiä, tarvitseeko kyseisessä projektissa suurempia datamääriä, kuin mitä Sigfox pystyy siirtämään, sillä Sigfoxin päivittäiset datamäärät, sekä datansiirtokyky on erityisen rajoitettu. [17.]

4.7 NFC

NFC, eli near-field communication on sarja langattoman yhteyden teknologioita. NFC:n erikoisuus on erityisen pienet osat, jotka saa helposti integroitua esimerkiksi matkapuhelimiin ja luottokortteihin. NFC:tä on otettu käyttöön esimerkiksi kauppojen kassoilla lähimaksamisen muodossa. Lähimaksamisessa maksupäätteen kyljessä on alue, jossa on NFC-sensori. Kun NFC:llä varustettu maksukortti tai puhelin, johon on liitetty maksukortti, tuodaan maksutilanteessa sensorin lähelle, maksun pystyy suorittamaan ilman kortin tunnuslukua. Korttia ei myöskään tarvitse laittaa maksupäätteen sisään. NFC:n kantama on erittäin lyhyt, maksimissaan noin 10 senttimetriä. NFC-yhteys toimii useimmiten lukija-luettava-mallilla. Tämä toimii esimerkiksi siten, että kortinlukija lukee luottokortissa olevasta NFC-sirusta maksukortti- tai kanta-asiakastiedot, tai muuta vastaavaa informaatiota.

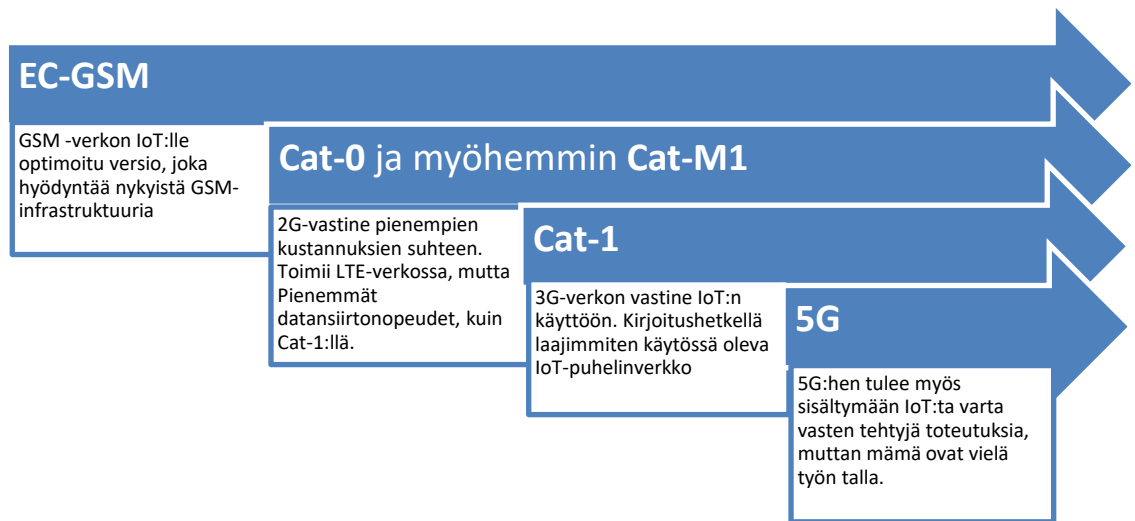
NFC:n tietoturva ei ole itsessään hyvällä tasolla. NFC ei juurikaan turvaa tiedonsiirtoa, ja sitä pystyykin salakuuntelemaan lyhyeltä etäisyydeltä. Laitteen käyttäjälle jää siis vastuu esimerkiksi liikenteen salaamisesta. Tästä huolimatta NFC:tä käytetään yleisesti luottokorteissa ja Suomessa maksutapahtumissa. Vaikka NFC-yhteyttä on mahdollista salakuunnella tai sen lähettämää dataa korruptoida, lyhyen kantaman vuoksi tämänlainen hyökkäys on vaikeaa toteuttaa. On kuitenkin ollut tapauksia, joissa taskussa olevilta korteilta on varastettu rahaa kortinlukijalla, joka toimi taskun ohuen kankaan läpi. NFC:n turvallisuutta varjostaa myös sitä käyttävien laitteiden ja esineiden pieni koko. Matkapuhelinten tai luottokorttien varastamisissa ei NFC:n tietoturvalla ole kovinkaan paljon merkitystä. Kun käyttötarkoituksen ja toteutuksen suunnittelee huolellisesti, on NFC varteenotettava teknologia lyhyen kantaman tiedonsiirtoon. [18.]

4.8 LTE Cat. M1, 0, EC-GSM, NB-IoT ja 5G

3GPP:llä on GSM-yhteyksien, kuten 2G, 3G ja 4G, lisäksi myös Internet of Thingsiä varten rakennettuja LTE-protokollia. Näitä protokollia on monia ja niiden suhde toisiinsa on hieman epäselvä. Vaikka 3GPP:n matkapuhelinverkkojen protokollat on tarkoitettu käytettäväksi matkapuhelimille, ne eivät ole tarpeeksi energiatehokkaita erittäin vähävirtaisille IoT-laitteille. Tästä syystä on kehitetty matkapuhelinverkkoja vastaavat IoT:lle tarkoitettut protokollat, jotka usein myös käyttävät samaa matkapuhelinverkon infrastruktuuria. Yleisellä tasolla kaikki IoT-puhelinverkot toimivat samalla periaatteella, kuin nykyiset mobiiliverkot, mutta erityisesti liikkuvuuteen, kantavuuteen, sekä energiatehokkuuteen on tehty parannuksia datan siirtonopeuden kustannuksella.

EC-GSM on 2G-puhelinverkon päällä toimiva IoT:lle optimoitu versio. Se pystyy 2G:n tavoin kuljettamaan ääntä, mutta sen vasteajat ovat suhteellisen korkeita verrattaessa muihin IoT-puhelinverkkoihin. EC-GSM on erityisen lupaava alueilla, joissa 2G on vahvasti tuettu, mutta 4G ei. Cat-1-verkko on tällä hetkellä jo käytössä oleva IoT-puhelinverkkototeutus. Se tukee 2G- ja 3G-varayhteyttä, jos 4G-verkko ei toimi alueella tarpeeksi hyvin. Cat-1 on tarpeeksi tehokas tukemaan puhetta yhteyden yli, joten se on tällä hetkellä lupaavalta vaikuttava ratkaisu myös terveydenhuollon piiriin. [19.]

Alkuaskeleilla olevia teknologioita on tällä saralla enemmän. Cat-0 on Cat-1:een verrattuna tarkoitettu pienemmille datamäärille, energiankulutukselle ja siten myös pienemmille laitteille, kuten erilaisille mittareille. Cat-0 on tarkoitettu asettamaan perustukset Cat-M1:tä, jonka arvellaan tuovan erittäin kustannus- ja energiatehokkaan valmiin LTE-infrastruktuurin päällä toimivan ratkaisun IoT-puhelinverkkoihin. NB-IoT hakee näitäkin enemmän energiatehokkuutta myyntivaltikseen, sillä sitä suunnitellaan käytettäväksi erittäin pienissä sensoreissa, jotka pysyvät elinkaarensa ajan paljolti samassa paikassa. Myös 5G:n roolia IoT:ssa pohditaan, mutta siitä ei kovin tarkkaa tietoa vielä ole, sillä se on vielä paljolti kehitysvaiheessa. 5G:n ensimmäisen vaiheen arvellaan julkaistavan alkuvuonna 2019. Sen kuitenkin odotetaan tuovan korkeampia datansiirtonopeuksia, sekä luotettavampaa yhteyttä, kuin edeltäjänsä. Tein näistä teknologioista rinnakkaisuutta selvittävän kuvan. [20.]



Kuva 3. 3GPP:n LTE-standardissa tulee olemaan monta hieman eri käyttötarkoitukseen suunnattua IoT-yhteysprotokollaa.

Tietoturvaan ei olla LTE-IoT -ratkaisujen kohdalla paljoa vielä perehdytty, sillä monet näistä teknologioista ovat vielä kehityksen alla. Tästä syystä monet tietoturvaa tarvitsevien ratkaisujen kanssa saa odottaa vielä näiden teknologioiden julkaisujen jälkeenkin, sillä tietoturvaongelmien löytämisessä voi mennä oma aikansa. Pienenä lohtuna voi arvioida, että koska nämä teknologiat ovat nykyisten mobiiliratkaisujen kanssa samankaltaisia, niiden tietoturvakuva voi myös vastata toisiaan. Tulee kuitenkin ottaa huomioon, että esimerkiksi energiatehokkuuteen tähdätessä, niissä on voitu myös tehdä kompromisseja tietoturvaan. [21.]

4.9 Thread

Thread on Googlen takaaman Nestin kodin automaatioon keskittyvä IoT-protokolla. Se on alusta alkaen rakennettu IoT:ia varten ottamalla huomioon muiden IoT-laitteiden puutteita, kuten tietoturvaa ja luotettavuutta. Thread voi toimia tilanteesta riippuen sähkölinjojen kautta, radiotaajuuksilla tai molemmilla. Se käyttää IP-protokollaa, joten esimerkiksi pilveen tai internetiin yhdistäminen on yksinkertaista. Thread salaa liikenteensä AES-salauksella. Vaikka Thread ei tarjoa julkisesti dokumentaatiota, ei sen käytöstä tarvitse maksaa lisenssimaksuja. Threadin käyttämiseen vaaditaan tosin erityisen laitetestauksen tekemistä, jotta se voidaan sertifioida Threadin hyväksymäksi. [22.]

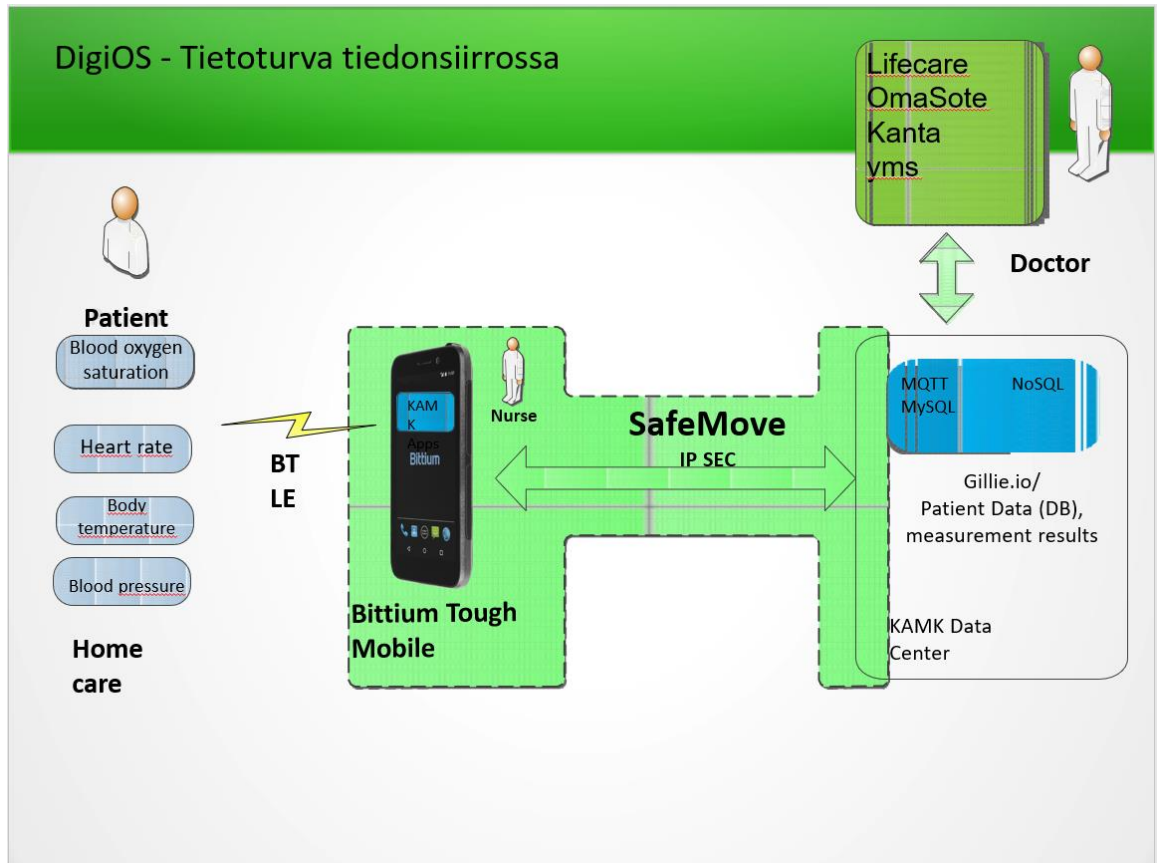
Googlen takaamana Threadilla on hyvät mahdollisuudet nousta laajemmaksi standardiksi IoT:n alalla. SANS Institutun tietoturvaselvityksestä käy ilmi, että tietoturvan alueella Thread on erityisen hyvä helppokäyttöiseen ja turvalliseen laitteiden yhdistämiseen ja salaamiseen. Vaikka nämä alueet on tehty Threadissa hyvin, jättää se esimerkiksi muun sovelluksen turvaamisen puolitiehen ja muiden vastuulle, eli Threadia käytettäessä sitä käyttävä ohjelmisto tulee myös turvata huolellisesti. Tämä on kuitenkin osittain sen syytä, että Thread on verkkoteknologia, eikä koko järjestelmä, eli muillakin IoT-teknologioilla on usein sama ongelma. [23.] [24.]

5. Case: DigiOS

DigiOS-hanke perustettiin kainuulaisten sosiaali- ja terveydenhuollon organisaatioiden digitaali- ja teknologiaosaamisen tarpeen vuoksi. Yhteiskunnan digitalisaatio ja teknologian kehittyminen muuttavat laajasti toimintamalleja niin yksityisen, kuin julkisen sosiaali- ja terveystalouden alueella. Hanketta hallinnoi Kajaanin Ammattikorkeakoulu ja sen arvioidaan valmistuvan toukokuun 2019 loppuun mennessä. Pää toteuttajana toimii Kajaanin Ammattikorkeakoulun sairaan- ja terveydenhoidon osaamisala, sekä osatoteuttajina Kainuun Sote, Kainuun Ammattiopiston hyvinvointiala, sekä Kajaanin Ammattikorkeakoulun tietojärjestelmät-osaamisala. [25.]

Hankkeen tavoitteena on Kajaanin Ammattikorkeakoulun mukaan kehittää pitkäaikaissairaiden asiakkaiden palvelujen asiakaslähtöisyyttä, sujuvuutta, vaikuttavuutta, sekä tehokkuutta uudistamalla hoito- ja palveluketju digitalisaatiota hyödyntäväksi kokonaisuudeksi. Tämä toteutetaan henkilöstön osaamisen kouluttamisen, opetussisältöjen uudistamisen, sekä digitalisaatio- ja teknologiaosaamiseen painottuvan koulutuspolun ja opetuksellisten demolaitteiden kehittämisen avulla. Konkreettisenä esimerkkinä hankkeessa on potilaiden aikaisempi kotiuttaminen mahdollistamalla heidän seuranta helppokäyttöisillä puhelimeen yhdistettävillä pienlaitteilla. Näillä laitteilla seurattaisiin esimerkiksi erilaisia elintoimintoja. Aikaisemman kotiuttamisen on todettu nopeuttavan paranemisprosessia, sillä sairaalaloissa stressitasot ovat monesti korkeammat, eli potilas rentoutuu helpommin kotioloissa.

Perustasolla järjestelmä tulisi toimimaan siten, että potilaalle annetaan kotikäyttöön esimerkiksi veren happisaturaatiota, sydämen lyöntitiheyttä, ruumiinlämpöä tai verenpainetta mittaavia laitteita. Näistä laitteista lähtisi Bluetooth Low Energyn avulla tiedot niihin liitettyyn Bittium Tough Mobile -matkapuhelimeen, josta tieto tallennetaan Bittiumin salatun SafeMove-yhteyden yli tietokantapalvelimille esimerkiksi Kajaanin Ammattikorkeakoulun konesaliin tai pilveen. Sieltä tiedot pystyttäisiin siirtämään OmaSoteen tai muuhun vastaavaan tietojärjestelmään. Terveydenhuollon järjestelmissä tietoturva on erityisen tärkeää varmistaa, eikä sen ratkaisu ole yksinkertaista. Siksi tämän kokonaisuuden jokaisen osan tietoturva pitää ottaa huomioon, sillä koko järjestelmä on vain heikoimman osansa vertainen.



Kuva 4. Yksinkertainen malli suunnitellusta järjestelmästä, jossa potilas saa kehon mittareita ja Tough Mobilen käyttöön, josta yhteys kulkee salattuna Gillie.io:n palveluun ja sieltä eteenpäin OmaSoteen ja Kajaanin Ammattikorkeakoulun pilveen. Lähde: DigiOS:n julkaisematon esitys. [26.]

Potilaalle annettavien laitteiden turvallisuudesta tulee tehdä selvitys, sillä laitteiden tietoturva jää useimmiten laitteen valmistajan vastuulle, eikä kaikkia ongelmia pystytä korjaamaan laitteen valmistuksen jälkeen. DigiOS:n suunnitelmassa halutaan käyttää Bittiumin Tough Mobile -matkapuhelinta, sekä yhdistää käytettäviin laitteisiin Bluetooth Low Energy -protokollaa käyttäen. Seuraavissa kappaleissa esittelen ja arvioin DigiOS:ssä käytettäviä teknologioita, sekä niiden tietoturva.

5.1 BLE

Bluetooth Low Energy, eli BLE on IoT:ssa suosittu protokolla, mutta sen käyttöönotossa tulee huomioida sen tuomat riskit. BLE:n versioissa on tietoturvan kannalta eroja. Bittium Tough Mobile tukee kirjoitushetkellä ainoastaan Bluetoothin 4.0 -versiota, jossa ei ole saatavilla uudempien versioiden tietoturvaparannuksia. Bluetooth 4.0:n yhdistämiskäytännössä kaikki liikenne liikkuu sa-

laamattomana, eli jos ulkopuolinen tekijä sattuu yhdistämishetkellä kuuntelemaan laitteiden sa-
lausavainten vaihtoa esimerkiksi langattomalla verkkoskannerilla, saa hän käsiinsä laitteiden käyt-
tämät avaimet. Näin hyökkääjän on mahdollista huijata laitteita ja ohjata kaikki laitteiden välillä
liikkuva liikenne oman laitteensa läpi.

Tämän haavoittuvuuden pystyy kuitenkin kiertämään yhdistämällä laitteet toisella tavalla. Lait-
teiden vaihtamat avaimet pystytään vaihtamaan myös Bluetooth-yhteyden ulkopuolella. Tällöin
puhutaan Out of Band Pairingista, eli kaistan ulkopuolisesta yhdistämisestä. Tämän voi toteuttaa
esimerkiksi erittäin lyhyen matkan NFC-yhteydellä. NFC-yhteydellä salakuuntelun mahdollisuus
on erittäin pieni, sillä sen kantama on vain muutamia senttejä. Näin tehtynä käyttäjä voi olla
varma, että yhdistetyt laitteet ovat juuri ne, jotka pitääkin. Samalla tavalla toimisi myös erillinen
numeronäyttö, josta voisi laitteiden välillä tarkistaa, että laitteet näyttävät samaa numeroa. [27.]

Sekä NFC, että numeronäytön toteutus vaatii laitteeseen lisää elektroniikkaa, jolloin hinta nousee
perusmalliin verrattuna. Etenkin numeronäyttö voi olla hankalaa toteuttaa pienillä laitteilla, joi-
den virransaanti ja koko on jo valmiiksi rajallista.

5.2 Bittium Tough Mobile

Bittium Tough Mobile on Bittiumin tekemä turvallisuus- ja kestävyyspainotteinen Android-poh-
jainen älypuhelin. Bittiumin mukaan Tough Mobile turvaa puhelimensa peukaloinnilta, sekä tur-
vaa käyttäjän yksityisyyden ja turvallisuuden. Kaikki puhelimen data on salattu, ja puhelin tarkis-
taa käynnistyksen yhteydessä ja käytön aikana puhelimen osien koskemattomuutta. Tämä kaikki
tieto on kuitenkin saatu heidän omilta sivuiltaan, joten sen voisi rinnastaa mainosmateriaaliin,
eivätkä he tarjoa tarkempia testejä yleisesti tarkasteltavaksi puhelimen tietoturvasta. Bittium on
myös sen verran pieni yritys maailmanlaajuisesti, ettei heidän puhelimiinsa ole helposti löydettä-
vissä tietoturva-analyyseja muilta tahoilta. Luottamusta kuitenkin tuo heidän maininnat siitä, että
Suomen puolustusvoimat käyttävät heidän tuotteitaan ja palveluitaan, mutta silti tarkempaa tie-
toa he eivät tarjoa. Heillä on tarjolla Tough Mobile C -paketti, johon kuuluu Tough Mobilen lisäksi
Bittium Secure Suite -ohjelmisto. Tough Mobile C on saanut viestintäviraston NCSA-FI -tietotur-
valuokituksen, joten sitä voi käyttää suojaustason III, eli luottamuksellisen tiedon kanssa. [28.]

Puhelin itsessään on kirjoitushetkellä jo hieman vanhentunut. Siinä on Android 6.0 -käyttöjärjes-
telmä, joka on julkaistu vuonna 2015 ja on kolme versiota uusinta jäljessä. Tietoturvapäivitysten
saaminen tälle laitteelle on hieman kyseenalaista, sillä esimerkiksi Google lopettaa oman vuonna

2016 julkaistun puhelimensa tietoturvapäivitysten tuen vuonna 2019. Ainoa maininta Bittiumin sivuilla päivityksistä on tieto, että päivitykset asennetaan automaattisesti. Tämä ei kuitenkaan vakuuta tuen jatkumisesta tulevaisuudessa, jos Bittium julkaisee uuden puhelimen tämän tilalle. Myöskään androidin versiopäivityksistä uudempiin ei löydy mitään tietoa. Versiopäivitysten mukana tulee usein myös tietoturvapäivityksiä, jotka muuten jäävät puhelimen tarjoajan vastuulle. Näistä puutteista huolimatta, suojaustason III käyttöön hyväksytyjen laitteiden ja järjestelmien tietoturvan pystyy mielestäni asettamaan myös terveydenhuollon käyttöön soveltuviksi, kunhan järjestelmän vaatimukset katsotaan asiantuntijan avulla tarkasti läpi. [29.] [30.] [31.]

5.3 SafeMove

Bittiumin SafeMove on VPN-yhteyden hallintajärjestelmä. Sen tarkoituksena on tarjota nopeasti yhdistävä ja vikasietoinen ratkaisu tietoturvalliseen tiedonsiirtoon erityisesti matkapuhelimille. SafeMoven koko ympäristöön kuuluu matkapuhelimille tarkoitettu Mobile VPN, laitteiden ja yhteyksien analysointiin tarkoitettu Analytics, katkeamattoman yhteyden turvaamiseen tarkoitettu Mobile Router Toolkit, sekä yksittäisten henkilöiden, esimerkiksi palomiesten, elintoimintoja monitorointiin tarkoitettu Zone. SafeMovea hallitaan keskeisestä hallintapaneelistä, ja sen pystyy konfiguroimaan erittäin automaattisesti, ettei loppukäyttäjän tarvitse itse kytkeä sitä päälle. Tämä on hyvä ratkaisu terveydenhuollon käyttöön, sillä se tekee loppukäyttäjän kokemuksesta helpompaa, eikä erityistä opettelua juurikaan vaadita.

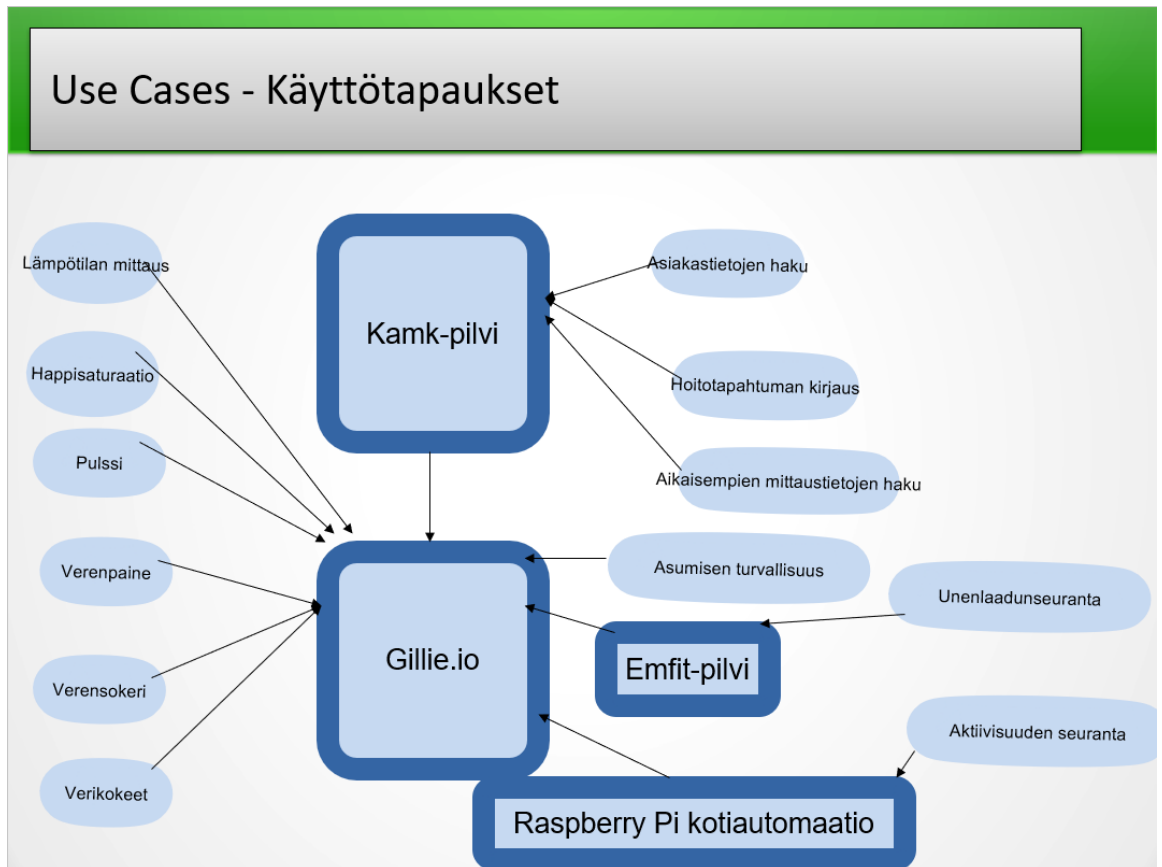
Bittiumin SafeMoven kanssa tilanne on hieman samankaltainen, kuin Tough Mobilen kanssa. Laajempia tietoturvatestauksia ei ole yleisesti saatavilla, joten lähteenä on ainoastaan Bittiumin tarjoama materiaali. Heillä on kokemusta sekä terveydenhuollon alalta että valtion toiminnoista, mutta käytännön esimerkkejä ja testituloksia ei ole helposti saatavilla. Oletettavasti he turvaavat omaa selustaansa, ja kertovat enemmän palveluistaan vain potentiaalisille asiakkaille suljettujen ovien takana. Tämä ei kuitenkaan poista epävarmuutta heidän tarjoamista tiedoista, sillä ulkopuolisia testejä heidän palveluistaan ei ole saatavilla.

5.4 Gillie.io, MQTT

Projektissa on tarkoitus käyttää Gillie.io:n tuotteita mm. verenpaineen, verensokerin, hemoglobiinin, painon ja kehonkoostumuksen mittaamiseen. Gillie.io:n keskittyminen vaikuttaa olevan

omien ratkaisujensa myynti muun, kuin verkon kautta, sillä heidän sivuillaan on erittäin vähän tietoa heidän toiminnastaan tai tarjoamistaan palveluista yksinkertaisia yleiskuvia lukuun ottamatta. Heidän tarjoamaan palveluun tulisi tehdä kunnollinen tietoturvaselvitys käyttämällä esimerkiksi OWASP:in tarjoamaa tietoturvatestien kehystä. Tällä hetkellä heidän järjestelmän tietoturva on täysin pimennossa. Jos he esimerkiksi tarjoavat verkosta ympäristön, josta tietoja voi tarkastella, täytyy kyseinen verkkoympäristön tietoturva testata ja turvata perinpohjaisesti, sillä talletettava data on melko varmasti arkaluontoista. Jokainen järjestelmän osa ja niiden väliset yhteydet pitää tarkistaa yleisimpien tietoturva-aukkojen varalta. Suunniteltu järjestelmä vaikuttaa monimutkaiselta, joten tämä tietoturvatestaus ja koventaminen tulisi teettää alan kokeneilla ammattilaisilla. [32.]

Paras tilanne olisi, jos mahdollisimman moni käytettävistä mittauslaitteista käyttäisi samaa verkoprotokollaa, mutta erilaisten datamäärien takia se ei välttämättä ole mahdollista. Muut yhteydet Gillie.io:n, Kajaanin Ammattikorkeakoulun pilven yms. välillä pitää myös salata. Raspberry Pi:n yhdistäminen tähän verkkoon on riski sen helppokäyttöisyyden vuoksi, mutta senkin tietoturvaa pystytään parantamaan. Root-käyttäjällä, eli Unixin tyyppisissä järjestelmissä pääkäyttäjällä, ei mielellään saisi ajaa ohjelmia, jos ei ole pakko. Mahdollisimman iso osa Raspberry Pi:lla olevasta datasta kannattaa laittaa vain-luku -tilaan, jolloin dataa ei pysty muokkaamaan. Yleisesti kaikki, mitä ei laitteella tarvitse, kannattaa ottaa pois, etenkin jos kyseinen ominaisuus mahdollistaa yhteyksiä mihinkään suuntaan, sillä monesti niissä piilee mahdollisuuksia hyökkäyksille. [33.]



Kuva 5. DigiOS-projektin kaavailtu kokonaisuus sisältää lukuisia erilaisia yhteyksiä ja järjestelmiä, joista kaikkien tietoturvariskit tulee ottaa huomioon. [26.]

MQTT, eli Message Queueing Telemetry Transport, on ISO-standardin mukainen viestiprotokolla, joka toimii TCP/IP:n päällä. Se noudattaa ns. julkaisija-tilaaja -mallia, jossa yksi julkaiseva laite on yhteydessä moniin tilaajalaitteisiin. Jokainen tilaaja tilaa topicin, eli aiheen, jolloin uuden viestin saapuessa julkaisijalle, se tarkistaa kaikki kyseisen viestin aiheen tilaajat ja lähettää viestin heille. Se on suunniteltu toimimaan pienellä jalanjäljellä, jolloin laitteet eivät kuluta paljoa suoritustehoa tai virtaa viestien liikuttamiseen. MQTT:n turvallisuus toteutetaan useimmiten viestien salaamisella, yhteyksien salaamisella tai erillisellä autentikointimekanismilla. Viestien ja yhteyksien salaamisessa tulee huomioida, että ne tuovat ylimääräistä tehtävää laitteen prosessorille, eikä kaikissa pienissä laitteissa välttämättä ole tarpeeksi suorituskykyä esimerkiksi TLS:n lisäämiseksi. TLS-versioissa kannattaa pysyä uusimmassa mahdollisessa, eikä käyttää SSL3:a tai vanhempaa ollelukaan, sillä niitä ei enää voi lukea tietoturvalisiksi. Julkaisijoilla kannattaa käyttää ulkopuolisesti allekirjoitettua sertifikaattia luotetulta sertifikaattien tarjoajalta. Tämä auttaa laitteiden yksilöinnissä ja estää ns. Man-in-the-Middle -hyökkäystä, sillä laitteet pystytään tunnistamaan sertifikaateilla. [34.]

5.5 MySQL, NoSQL

DigiOS:n käytössä on kaksi erilaista tietokantamallia, MySQL-relaatiotietokanta, sekä MongoDB, joka ei käytä kiinteästi määrättyä taulukkoskeemaa, vaan on ns. NoSQL-tietokanta. Molemmat täytyy koventaa erikseen, sillä tietokantoihin tallennetaan terveydenhuollon tietoja, jotka ovat oletettavasti arkaluontoista. Käytettävien tietokantojen salaus, pääsyn hallinta, datan validointi tulee siis ottaa huomioon.

Yleisenä nyrkkisääntönä tietokannoissa on, että ne eivät saa olla suorassa yhteydessä internetiin, sillä se avaa suurimman hyökkäyspinnan vihamielisille osapuolille. Ohjelmistopäivitykset tulee pitää ajan tasalla, eikä tietoturvapäivityksiä saa laiminlyödä. Tietokannoissa ja niiden tietokoneilla tulee olla erittäin vahvat salasanat, joissa on aakkosten lisäksi numeroita ja erikoismerkkejä. Tämä on helppoiten toteutettavissa salasanageneraattorilla. Erytishuomiota täytyy kiinnittää MySQL-tietokannan root-käyttäjään, jolle täytyy erikseen määrittää salasana. Käyttäjienhallinnassa tulee noudattaa vähimmän oikeuden sääntöä, englanniksi The Rule of Least Privilege. Tämä tarkoittaa sitä, että kaikille käyttäjille annetaan vain tarvittavan suuret oikeudet, eikä yhtään enempää. Näin käyttäjillä ei ole pääsyä paikkoihin, joihin heidän ei tarvitse koskea, mikä rajaa samalla mahdollisissa murtotilanteissa vahinkojen laajuutta. [35.] [36.]

Tietokantoihin pääsy kannattaa myös rajoittaa vain tietyille tietokoneille tai jopa ainoastaan yhdelle fyysiselle hyvin turvatulle tietokoneelle, sillä tämä pienentää mahdollista hyökkäyspintaa. Tietokantaan tulisi yhdistää ainoastaan salatulla yhteydellä, ettei verkkoliikennettä kuunteleva taho saa selväkielisenä mitään verkossa liikkuvaa tietoa. Tietokantaan laitettava tieto voidaan myös salata, ettei mahdollisen tietomurron yhteydessä arkaluontoista tietoa joudu väärin käsiin selväkielisenä.

5.6 Terveydenhuollon vastuhenkilö

Potilaita ei jätetä IoT:n tuomien hyötyjen jälkeenkään yksin, vaan terveydenhuollon puolelta löytyy tätä varten vastuhenkilö. Tälle vastuhenkilölle täytyy kouluttaa kaikkien potilaalle annettavien laitteiden käyttö ja yksinkertainen vianselvitys. Vastuhenkilön olisi hyvä olla muutenkin perustason puhelimen ja sen lisälaitteiden käyttö hallussa, sillä monet tämän projektin tuomista laitteista ovat huomattavasti helppokäyttöisempiä, jos tuntee muita puhelimen lisälaitteita. Vastuhenkilö myös ohjeistaa potilaita laitteiden käytössä. Tämä voi olla yllättävän haastavaa, sillä

etenkin vanhemmat potilaat eivät välttämättä osaa käyttää älylaitteita ollenkaan, jolloin hyvä ja selkeä ohjeistus on elintärkeää. Voi myös olla, että tietty tekniikan taito olisi vaatimuksena, että kotihoitoon laitteiden avustuksella pääsee.

Myös ongelmatilanteet laitteiden kanssa tulee ottaa huomioon, sillä hajonneet tai väärää tietoa lähettävät laitteet ovat suuri riski potilaan hyvinvoinnille, jos esimerkiksi potilaan huononevaa tilaa ei huomata. Tästä syystä koulutuksessa tulee myös käydä läpi mahdollisten vikatilanteiden huomaaminen laitteiden lähettämästä datasta. Potilaan kanssa yhteydenpito on sanomattakin selvää

Tietoturvasta itsestään henkilöstöä tulee kouluttaa oikeaoppisesta laitteiden asennuksesta ja käyttöönotosta, sillä esimerkiksi joissain verkkoprotokollissa käyttöönottovaiheessa ilmenee suurimmat tietoturvariskit, jos erityisiä varotoimenpiteitä ei tehdä. Laitteiden yhdistämisessä täytyy olla tarkkana, että yhdistetty laite on juuri se, joka sen pitääkin olla. Varmentamista voi helpottaa esimerkiksi numeronäyttö, jolla laitteet voivat näyttää käyttäjälle toisiaan vastaavan koodin. Järjestelmiin oletettavasti kirjaudutaan henkilökohtaisilla tunnuksilla, jolloin tunnusten salasanaikäytäntö pitää myös olla kunnossa, ettei tietoihin pääse käsiksi liian heikolla salasanalla. Riippuen tilanteesta, järjestelmään pääseviä laitteita voi myös rajoittaa esimerkiksi pelkästään terveydenhuollon IT:n piirissä oleviin tietokoneisiin tai vielä tarkemmin tiettyjen henkilöiden laitteisiin. Avoimesta internetistä ei mielellään saisi olla pääsyä järjestelmiin edes tunnuksilla, sillä se avaa valtavan riskin salakuunteluun, sillä ulkoisten laitteiden varmentaminen on mahdotonta.

6. Yhteenveto

Internet of Thingsin tietoturvaan ei ole yksinkertaista ratkaisua. IoT:n ala kattaa niin suuren määrän laitteita ja käyttötarkoituksia, että kaikenkattavaa ratkaisua on tällä hetkellä mahdoton tehdä. Jos IoT:n laitteita halutaan käyttää projekteissa, on suositeltavaa tehdä huolellista selvitystyötä tarjolla olevien ratkaisujen ominaispiirteistä, vaatimuksista ja rajoitteista, jotta välttyttäisiin ylimääräisiltä kustannuksilta tai pahimmillaan projektien kariutumisilta. Verkossa on hyvin tietoa yleisimmistä verkkostandardeista perustasolla, mutta tarkempaa tietoa voi joutua kyselemään valmistajilta tai protokollaa hallinnoivalta taholta.

Tietoturva on iäti jatkuvaa kilpavarustelua hyökkääjien ja puolustajien välillä, sillä täysin varmaa järjestelmää ei ole olemassa. Laitteita, järjestelmiä ja käytettäviä teknologioita valittaessa riskikartoitus on tärkeää, jotta helpoimmin korjatut ja hyväksikäytetyt heikkoudet saadaan paikattua. Jossain vaiheessa turvaamisen kustannukset nousevat yli järkevän tason, mutta silloin täytyy hyväksyä voimassa olevat riskit, sekä huolehtia riskienhallinnan toiminnot kuntoon.

DigiOS-projekti pyrkii tuomaan IoT-laitteet terveydenhuollon piiriin mahdollistamaan potilaiden kotihoidon entistä aikaisemmin. Tähän päästään rakentamalla tietoturvallinen terveydenhuollon piiriin sopiva järjestelmä tiettyjen elintoimintojen seuraamiseksi, jotta potilas pystyy tekemään sen itsenäisesti tai pienellä avustuksella kotoa käsin. Tämän tavoitteena on nopeuttaa potilaiden kotiutumista, jonka on todettu nopeuttavan paranemisprosessia.

Gillie.io:n ratkaisumallissa esimerkiksi veren happisaturaatiota, sydämen lyöntitiheyttä, ruumiinlämpöä tai verenpainetta mittaavia laitteita käytetään Bittiumin Tough Mobilen kanssa. Tästä tietoturvaan keskittyvästä älypuhelimesta olisi salattu yhteys Kajaanin Ammattikorkeakoulun kone-saliin ja terveydenhuollon palveluihin. Koska tämä järjestelmä tulisi käyttöön terveydenhuollon alalle, on tietojen käsittelyn turvaaminen erittäin tärkeää, sillä monesti kyseessä on arkaluontoista tietoa. Ratkaisumallissa on paljon eri laitteita, joista jokaisen kohdalla täytyy tietoturvaa ja riskejä arvioida erikseen, sillä oikeittejä ei ole.

Lähteet

1. Columbus L. 2017 Roundup Of Internet Of Things Forecasts [Internet]. 2017; Saatavilla: <https://www.forbes.com/sites/louiscolombus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#2340c7dc1480>
2. Adafruit Industries. 35750892571 , PyCom SiPy 1.0 – ESP32 WiFi, BLE and +22dBm SigFox Radio [Internet]. 2017. Saatavilla: <https://www.flickr.com/photos/adafruit/35750892571>
3. Brigance Y. Wifi vs Bluetooth vs BLE, choosing the right IoT tech [Internet]. 2017; Saatavilla: <https://appdeveloper magazine.com/wifi-vs-bluetooth-vs-ble,-choosing-the-right-iot-tech/>
4. Suthers E. Wi-Fi Alliance introduces low power, long range Wi-Fi HaLow? 2016; Saatavilla: <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow>
5. Zeus K. Why 802.11ax is the next big thing in Wi-Fi. 2018; Saatavilla: <https://www.networkworld.com/article/3215907/mobile-wireless/why-80211ax-is-the-next-big-thing-in-wi-fi.html>
6. Peterson M. GSM / 3G / 4G (LTE) - Which One to Choose for Your IoT Project? 2017; Saatavilla: <https://1ot.mobi/blog/gsm-3g-4g-lte-which-one-to-choose-for-your-iot-project>
7. Elisa. Elisa Kuuluvuuskartta, haettu syksyllä 2018. Saatavilla: <https://elisa.fi/kuuluvuus/>
8. Gallagher S. LTE security flaws could be used for spying, spreading chaos [Internet]. 2018; Saatavilla: <https://arstechnica.com/information-technology/2018/03/even-more-bugs-in-lte-networks-allow-eavesdropping-fake-emergency-messages/>
9. Engineers garage. Difference between Bluetooth and Zigbee Technologies . 2016; Saatavilla: <https://www.engineersgarage.com/contribution/zigbee-vs-bluetooth>
10. Fan X, Susan F, Long W, Li S. Security Analysis of Zigbee. 2017. <https://courses.csail.mit.edu/6.857/2017/project/17.pdf>

11. Idbivanov. Ransomware and Your Smart Home – The Security of Z-Wave. 2017; Saatavilla: <https://buildyoursmarthome.co/home-automation/protocols/security-of-z-wave-protocol/>
12. Z-Wave Alliance. Mandatory Security Implementation for All Z-Wave Certified IoT Devices Takes Effect Today. 2017; Saatavilla: <https://z-wavealliance.org/mandatory-security-implementation-z-wave-certified-iot-devices-takes-effect-today/>
13. Poole I. SIGFOX for M2M & IoT. Haettu syyskuu 2018; Saatavilla: <https://www.radio-electronics.com/info/wireless/sigfox/basics-tutorial.php>
14. HidnSeek. Sigfox world record distance transmission. 2017; Saatavilla: <https://twitter.com/xtorrest/status/895583422130798593>
15. Meyerb KM Eddy Bajica, Frederic Chaxela, Fernand. A comparative study of LPWAN technologies for large-scale IoT deployment. 2018; Saatavilla: <https://www.sciencedirect.com/science/article/pii/S2405959517302953>
16. WNDgroup. What makes Sigfox so secure for the Internet of Things? 2017; Saatavilla: <https://www.wndgroup.io/2017/09/18/sigfox-security-internet-things/>
17. Sigfox. Make things come alive in a secure way. Saatavilla: <https://www.sigfox.com/en/technology/security>
18. Communication NF. Security Concerns with NFC Technology. 2017; Saatavilla: <http://nearfieldcommunication.org/nfc-security.html>
19. u-blox. LTE Cat 1. 2018; Saatavilla: <https://www.u-blox.com/en/lte-cat-1>
20. Vos G. What is LPWA for the Internet of Things? Part 3: A Guide to Decoding the Technologies. 2018; Saatavilla: https://www.sierrawireless.com/iot-blog/iot-blog/2016/08/lpwa_for_the_iot_part_3_a_guide_to_decoding_lpwa_technologies/
21. Hwang Y. Cellular IoT Explained: NB-IoT vs. LTE-M vs. 5G and More. 2018; Saatavilla: <https://medium.com/iotforall/cellular-iot-explained-nb-iot-vs-lte-m-vs-5g-and-more-8f26496df5d4>
22. Lynnette Reese M. Choosing the best IoT protocol. 2016; Saatavilla: <http://www.embedded-computing.com/embedded-computing-design/choosing-the-best-iot-protocol>

23. Strayer K. Can the “Gorilla” Deliver? Assessing the Security of Google’s New “Thread” Internet of Things (IoT) Protocol [Internet]. STI Graduate Student Research; 2017. Sivut 3-6, 23-24. Saatavilla: <https://www.sans.edu/cyber-research/white-papers>
24. Seven keys to understanding Thread protocol. 2016; Saatavilla: https://www.electronicproducts.com/Digital_ICs/Communications_Interface/Seven_keys_to_understanding_Thread_protocol.aspx
25. Ammattikorkeakoulu K. DIGIOS – Digitaalisen osaamisen kehittäminen sosiaali- ja terveydenhuollon koulutuksessa ja palveluissa Kainuussa [Internet]. Saatavilla: <http://web1.kami.fi/digios/hanke/>
26. Kuva DigiOS:n julkaisemattomasta esityksestä. Värejä muokattu paremman luettavuuden vuoksi.
27. Bon M. A Basic Introduction to BLE Security [Internet]. 2016. Saatavilla: <https://www.digikey.com/eewiki/display/Wireless/A+Basic+Introduction+to+BLE+Security#ABasicIntroductiontoBLESecurity-SecurityIssuesFacingBLE>
28. Bittium. Bittium Tough Mobile? - Secure and strong LTE smartphone [Internet]. Saatavilla: <https://www.bittium.com/BittiumToughMobile>
29. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot . Sivut 2-5. Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Kryptografiset_vahvuusvaatimukset_-_kansalliset_suojaustasot.pdf
30. Viestintävirasto. Ohje arviointikriteeristöjen tulkinnasta. 2015; Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Ohje_arviointikriteeristojen_tulkinnasta.pdf
31. Google. Android-päivitysten aikataulut Pixel-puhelimilla ja Nexus-laitteilla. Saatavilla: https://support.google.com/nexus/answer/4457705?visit_id=636781525942383063-3225992418&rd=1
32. Gillie.io. Healthcare AI platform. Saatavilla: <http://www.gillie.io/features.html>
33. Hardening the Raspberry Pi [Internet]. 2014. Saatavilla: <https://www.raspberrypi.org/forums/viewtopic.php?t=115768>

34. Hivemq. MQTT Security Fundamentals: TLS / SSL. 2016; Saatavilla: <https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl>
35. Rankin K. 5 Essential Steps to Hardening Your MySQL Database. 2017; Saatavilla: <https://medium.com/linode-cube/5-essential-steps-to-hardening-your-mysql-database-591e477bbbd7>
36. Krug P. NoSQL, no problem: securing non-relational databases. 2018; Saatavilla: <https://www.scmagazineuk.com/nosql-no-problem-securing-non-relational-databases/article/1473483>