Milla Jämsen

Esineiden internetin hyödyntäminen terveydenhoidossa ja tartuntatautien hallitsemisessa

Tietotekniikan kandidaatintutkielma

8. toukokuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Milla Jämsen

Yhteystiedot: milla.k.jamsen@student.jyu.fi

Ohjaaja: Leevi Annala

Työn nimi: Esineiden internetin hyödyntäminen terveydenhoidossa ja tartuntatautien hallitsemisessa

Title in English: Usage of Internet Of Things in healthcare and in fight against infectious diseases

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 30+0

Tiivistelmä: Esineiden internet eli the internet of things (IoT) on yksi uusista teknologioista, joita voidaan soveltaa terveydenhoidossa ja tartuntatautien torjumisessa. Sen avulla voitaisiin potentiaalisesti nostaa terveydenhoidon tasoa. Ensin tässä tutkielmassa tarkastellaan IoT-laitteita yleisesti, niissä käytettyjä yleisiä teknologioita ja ehdotettuja arkkitehtuureja. Seuraavaksi tutkitaan esineiden internetiä terveydenhoidossa (engl. *Internet Of Healthcare Things*) (IoHT). Sitten vielä katsotaan IoHT:ta tartuntatautien kontekstissa. Lopuksi pohditaan eettisiä kysymyksiä ja tietoturvaongelmia.

Avainsanat: esineiden internet, kontaktien jäljitys, lääketieteellisten esineiden internet

Abstract: The Internet of things (IoT) is one of the emerging technologies concerning healthcare and fighting infectious diseases in recent times. New technology has a lot of potential to upgrade medical care. This thesis examines the mentioned topic from multiple points of view. First we look at IoT in general, next we look at the Internet of healthcare things also known as IoHT. Then we examine IoHT specifically from the perspective of infectious diseases. Finally we take a look at cybersecurity and ethical concerns within IoT.

Keywords: Internet of things, contact tracing, internet of healthcare things, epidemic detection

Termiluettelo

kontaktien jäljitys	(engl. *contact tracing*) sairastuneen henkilön lähellä, yleensä tietyllä etäisyydellä, olleiden ihmisten kartoitus.
data	kerättyä informaatiota liittyen johonkin asiaan.
terveysdata	viittaa henkilökohtaiseen tietoon, joka liittyy henkilön terveydentilaan.
massadata	(engl. *big data*) suuri määrä jatkuvasti lisääntyvää dataa eri lähteistä. Termiin liittyy myös datan käsittely ja analysointi.
internet	tietoverkkojen tietoverkko, jossa tietotekniset laitteet ovat yhdistetty toisiinsa internetprotokollalla.
epidemia	laajalle levinnyt esiintymä tarttuvaa tautia tietyssä yhteisössä tiettynä aikana (Zgheib ym. 2020).

Kuviot

Taulukot

Sisällys

1 Johdanto

Viimeaikainen edistys mobiili-, sensori- ja tekoälytekniikassa mahdollistaa täysin uudenlaisen lähestymistavan sairaanhoitoon terveydenhoidon monella eri osa-alueella. Erilaiset välineet, joilla on sisäänrakennettu ominaisuus olla yhteydessä joko yleiseen internetiin tai muuhun verkkoon ja näin lähettää tietoa itsestään ulkomaailmaan voivat vähentää terveydenhuollon kustannuksia samalla nostaen sen tasoa ja joustavuutta (Rahmani ym. 2018). Erinäisten terveydehuollon osa-alueiden ongelmien ratkaisuiksi voidaan kehitellä systeemejä koostuen erilaisista sensoreista, älylaitteista, pilvipalveluista ja muista mahdollisesti tarvittavista osasista. Internetiin yhteydessä olevista laitteista koostuvista järjestelmistä käytetään akronyymia IoT (lyhenne eng. sanoista *Internet of Things*), josta suomeksi käytetään termiä *esineiden internet*.

Oikein implementoituna IoT-ratkaisuista voi olla paljon hyötyä. Potilaiden yleistilasta voidaan saada täydellisempi kuva, sairaalassa vietetty aika vähenee, itsehoitokeinot monipuolistuvat ja sairaalahoidosta tulee entistä tehokkaampaa. Toisaalta haasteita IoT-laitteiden käyttöönotossa ovat standardien puute (Ahmadi ym. 2019), akun kesto laitteissa (Selvaraj ja Sundaravaradhan 2020), tietoturvallisuus äärimmäisen arkaluontoisen terveysdatan käsittelyssä (Strielkina ym. 2018) ja tästä seuraava ihmisten epäluuloisuus IoT-laitteita kohtaan (Mittelstadt 2017).

Erilaisten tartuntatautien leviäminen on yleinen ongelma, johon liittyy useampia ulottuvuuksia. Voidaan tarkastella suljettuja tiloja, kuten sairaaloita tai lentokenttiä, mutta myös ihmisten liikkuminen laajalla alalla paikasta toiseen voi olla kiinnostavaa. Nykyään globalisaation tuloksena ihmisten liikkuvuus on suurta, mikä luo täysin uudenlaisia haasteita epidemiologisesta näkökulmasta. Tuntemattomilla uusilla taudinaiheuttajilla on ennennäkemättömät mahdollisuudet nopeaan leviämiseen ihmisten keskuudessa. Myös ilmastonmuutos aiheuttaa trooppisten alueiden tartuntatautien leviämistä yhä laajemmalle alueelle (Eckhardt ym. 2020). Tartuntataudeilla tässä tutkielmassa tarkoitetaan kaikkia sellaisia tauteja, jotka tarttuvat joko ihmiseltä ihmiselle, ihmiseltä pinnalle tai pinnalta ihmiselle. Tällaisia tauteja ovat esimerkiksi COVID-19, ebola, SARS (lyhenne eng. sanoista *Severe acute respiratory syndrome*), MERS (lyhenne eng. sanoista *Middle East respiratory syndrome*) tai kausifluns-

sa. Kuitenkaan tämä tutkimus ei tarkastele vain yhtä taudinaiheuttajaa, vaan pyritään kartoittamaan laajaa ja yleishyödyllistä tapaa tartuntatautien ehkäisyyn IoT-teknologian avulla.

Uutta tutkimusta aiheesta on tarpeellista tehdä, koska tietoa uusien teknologioiden soveltamisesta tehokkaasti ja tarkoituksellisesti tarvitaan uusien globaalien terveysriskien ratkaisuun. Tietenkin aihe on ajankohtainen juuri nyt COVID-19-pandemian takia, mutta myös paljon tarpeellista infrastruktuuria niin globaalin kuin pienemmänkin skaalan valvontajärjestelmän toteuttamiseksi on jo toiminnassa enemmän kuin koskaan, jota voitaisiin mahdollisesti soveltaa kyseiseen tarkoitukseen (Rahman ym. 2020).

Tutkimuksia, jotka kokoaisivat yhteen esineiden internetin, näiden sovellukset terveydenhoidossa ja tartuntataudit, ei juurikaan vaikuta olevan tehty. Laajoja kirjallisuuskatsauksia liittyen IoT:hen ja IoT-sovelluksiin terveydenhuollossa löytyy, mutta tartuntatautien kontekstista löytyy pienempiä tutkimuksia yleensä sidottuna johonkin tiettyyn tautiin ja sen leviämisen mallinnukseen tarjoten IoT-pohjaisen ratkaisun sen hillitsemiseen. Kanditutkimuksen tavoitteena on tarkastella näitä kaikkia yleisellä tasolla ja luoda kokonaiskuva johtavasta tekniikasta IoT:n parissa.

Tämä tutkielma koostuu kahdeksasta luvusta. Toisessa luvussa esitellään IoT-teknologiaa yleisesti, kolmannessa luvussa esitellään IoT terveydenhuollon näkökulmasta ja neljännessä IoT-ratkaisuja tartuntatautien leviämiseen. Viidennessä kappaleessa käsitellään Google flu trends -projektia ja sen epäonnistumista. Kuudennessa kappaleessa käsitellään kyberturvallisuutta IoT-laitteissa. Seitsemännessä kappaleessa käsitellään eettisiä ongelmia liittyen terveydenhuollon IoT-ratkaisuihin. Kahdeksannessa kappaleessa on yhteenveto tutkielman aiheista ja pohdintaa hyötyjen ja haittojen suhteesta.

2 Esineiden internet

Esineriden internet (engl. *internet of things*) (IoT) viittaa useimmiten esineisiin ja asioihin, jotka ovat yhteydessä ihmisiin ja toisiin esineisiin verkon yli, jakaen tietoa itsestään ja/tai ympäristöstään Ne myös voivat osata organisoida ja lajitella omaa dataansa, reagoida muuttuneeseen ympäristöönsä tai tilanteeseensa (Madakam ym. 2015). Internet of things-käsitteelle ei kuitenkaan ole yhtä tarkkaa määritelmää. Tyypillisesti IoT-laitteet kuvitellaan sellaisiksi jokapäiväisiksi esineiksi ja asioiksi, joita ei tyypillisesti yhdistetä tietotekniikkaan, kuten esimerkiksi jääkaappi, lamput tai leivänpaahdin.

IoT-laitteisiin yleensä liitetään myös käsite teknologiasta, joka sulautuu ympäristöönsä (Madakam ym. 2015). Tämä tarkoittaa sitä, että esineiden käyttäjät tai samassa tilassa esineiden kanssa olevat eivät välttämättä heti ensisilmäyksellä osaa sanoa ovatko heidän käyttämänsä laitteet tai huoneessa olevat esineet yhteydessä verkkoon.

IoT-laitteille ei ole olemassa yhtä hyväksyttyä arkkitehtuurimallia, mutta useita ehdotettuja arkkitehtuurimuotoja on esitetty. Useimmiten ehdotetaan kerrosarkkiehtuuria, koska siinä on monia käytännöllisiä ominaisuuksia. Kerrosarkkitehtuurit ovat myös yleisesti käytössä internetissä. Esimerkiksi TCP/IP-viitemalli, joka kuvaa internetin kuljetuspalvelua, mielletään koostuvan useasta kerroksista (Cerf ja Kahn 1974). Kerrosarkkitehtuuri tarkoittaa sitä, että laitteen tiedon käsittely on jaettu kerroksille. Jokaisella kerroksella on oma toimintansa, joka pyritään toteuttamaan niin että se olisi mahdollisimman eristetty muiden kerrosten toiminnasta. Toisin sanoen kerrokset ovat kapseloituja. Jokainen kerros tarjoaa palvelunsa käyttöön rajapinnan kautta sitä ylemmälle kerrokselle niin että ylemmän kerroksen ei tarvitse huolehtia alemman sisäisestä toteutuksesta. Eri laitteissa sijaitsevat saman kerroksen toteutukset kommunikoivat yhteisellä protokollalla. Kerrosarkkitehtuurin hyvä puoli on se, että yksittäisiä kerroksia on helppo kehittää, sillä yhden kerroksen toteutuksen muokkaaminen ei vaikuta muihin kerroksiin.

IoT-laitteille on yleensä ehdotettu 3 - 5 kerroksista arkkitehtuuria (Lu ja Da Xu 2018). Voidaan tarkastella tässä esimerkkinä nelikerroksista arkkitehtuuria johon kuuluu havaintokerros, verkkokerros, palvelukerros ja käyttöliittymäkerros (Li ja Da Xu 2017) (sivu 6). Tässä

siis havaintokerros on alimmainen ja käyttöliittymäkerros ylimmäinen kerros.

- Havaintokerros (engl. *Sensing layer*) sisältää laitteiston ja protokollat jotka keräävät datan. Esimerkiksi bluetooth, RFID tai muut sensorit ja niihin liittyvät protokollat. Näitä käsitellään tarkemmin myöhemmin tutkielmassa.
- Verkkokerros (engl. *network layer*) tai gateway layer kerää dataa yhdestä tai useammasta laitteesta ja lähettää ne eteenpäin internetin yli.
- Palvelukerros (engl. *service layer*) tarjoaa asiakkaan tai muun käyttäjän tarvitseman toimintalogiikan, eli se muokkaa saamansa datan sellaiseen muotoon, joka on hyödyllinen käyttäjille. Kyseessä on usein pilvipalvelu.
- Käyttöliittymäkerros (engl. *interface layer*) on kerros, joka jollain tapaa näyttää tai ilmoittaa käsitellyn datan loppukäyttäjälle.

Madakam ym. (2015) kuvaa vaatimuksia onnistuneeseen IoT-laitteiston käyttöönottoon seuraavanlaiseksi: asiakkaalla on tarve saada tietoa dynaamisesti eri lähteistä ja tiedon tulee olla lähes reaaliaikaista. Laitteistolle tulee olla myös kysyntää ja sopivia sovelluksia tulee olla saatavilla. Teknisellä tasolla laitteiston kyberturvallisuuden tulee olla sopivalla tasolla, sen energiankulutus tulee olla mahdollisimman pientä ja sen pitää sijaita käyttäjiensä lähettyvillä. Käytännössä myös tarvitaan jokin pilvipalvelu, joka soveltuu latteen käyttöön.

2.1 Teknologiat

IoT-laitteiden toteutukseen liittyy useampia avainteknologioita, joita ilman ne eivät olisi mahdollisia. Näistä keskeisin on RFID (lyhenne engl. sanoista *radio frequency identification*) (Madakam ym. 2015). RFID-tunniste on pieni siru, joka sisällytetään esineeseen tai asiaan. RFID-tunniste voi sisältää suuriakin määriä tietoa. Juuri tämä on yksi RFID:n eduista verrattuna viivakoodeihin, joihin tallennetun tiedon määrä on rajattu. RFID:n toiminta perustuu radiosingnaalieihin, joita lukija-laite vastaanottaa tunnisteelta ja muuntaa digitaaliseksi tiedoksi. Tunnisteen ja lukijan siis ei tarvitse olla fyysisessä kontaktissa (Finkenzeller 2010)(kappale 1.1.5). RFID-tunnisteet ovat tuttuja kaupoista, jotka lisäävät tuotteisiinsa varkaudenesto-tunnisteen, joka laukaisee hälytyksen, jos se kuljetetaan ulos kaupan ovien vieressä olevien porttien välistä. Tässä tapauksessa portit ovat siis skannereita.

EPC (lyhenne engl. sanoista *electronic product code*) on uniikki koodi, joka on RFID-tunnisteen sisällä. Se voi sisältää kaikenlaista dataa esineestä. Data on bitteinä, ja tällä hetkellä EPC-koodi voi olla joko 64 tai 96 bittiä pitkä (Finkenzeller 2010) (kappale 9.6.3.2).

Bluetooth on myös yksi keskeisistä teknologioista IoT-laitteiden sovelluksissa. Yleisesti bluetooth-teknologiaa käytetään korvaamaan johdot laitteiden välillä lyhyellä etäisyydellä. Myös bluetooth käyttää radioteknologiaa yhteyksien luomisessa. Laitteisiin, jotka halutaan yhdistettävän toisiinsa lisätään siru, joka kykenee lähettämään ja vastaanottamaan datapaketteja ("about bluetooth" 2021). IoT-sovelluksissa yksi haasteista on laitteiden energiankulutus. Bluetooth low-energy (BLE) on kehitetty ratkaisuksi laitteisiin jotka toimivat pattereilla tai joiden kommunikointi ei tapahdu usein (Chang 2014).

GPS (lyhenne engl. sanoista *Global Positioning System*) on satelliitteihin ja niiden lähettämiin mikroaaltoihin perustuva paikannusjärjestelmä. Se tarjoaa IoT-laitteille mahdollisuuden tietää oman sijaintinsa missä tahansa maapallolla. GPS mahdollistaa myös sijaintihistorian tallentamisen. Vastaanottolaite laskee vähintään neljän GPS-satelliitin sijainnin ja niiden lähettämän signaalin viiveen perusteella oman sijaintinsa kolmiulotteisessa avaruudessa. Myös vastaanottolaitteen kiihtyvyys voidaan määrittää näin. GPS-paikannus vaatii että vastaanottolaitteessa on kello. Neljän satelliitin vaatimus perustuu siihen että tarvitaan vastaanottajan pituusaste, leveysaste, korkeus ja laitteen kellon virhe. Jos jotkin näistä arvoista on jo tarkasti tiedossa, voidaan käyttää vähemmän kuin neljää satelliittia mikä tehostaa toimintaa. (Kaplan ja Hegarty 2005) (sivu 3)

Mobiiliteknologian tiedonsiirto on tällä hetkellä siirtymävaiheessa neljännen ja viidennen sukupolven matkapuhelinverkon välillä. Niin kutsuttu 5G-teknologia tarjoaa entistä paremmat puitteet esineiden internetille ja sen ennustetaan laajentavan IoT:n sovellusalaa huomattavasti. 5G tarjoaa jopa noin kymmenkertaisen tiedonsiirtonopeuden 4G:hen verrattuna. Se myös vähentää viiveaikaa, nostaa verkon kapasiteettia eli verkossa olevien laitteiden maksimimäärää, vähentää virrankulutusta, nostaa tietoturvallisuuden tasoa ja parantaa verkon luotettavuutta (Gupta ja Jha 2015). 5G tajoaakin moneen esineiden internetiin liittyvään haasteeseen ratkaisun ja on varmasti yksi osasyy sille, miksi IoT-laitteiden käyttö tulee luultavasti kasvamaan tulevina vuosina. Matkapuhelinverkkon laajan kuuluvuusalueen takia IoT-laitteiden käyttö tulee mahdolliseksi turvallisesti ja luotettavasti syrjäisemmilläkin alueilla.

Lisäksi verkon luotettavuuden takia IoT-teknologiaa voitaisiin hyödyntää entistä laajemmin kriittisissä infrastruktuureissa ja tilanteissa, kuten kirurgisissa operaatioissa, joissa verkkoyhteyden on oltava vakaa.

teknologia	sähkön kulutus	tiedonsiirtonopeus	signaalin etäisyys
RFID	keskitaso	40-640 Kb/s	100 m
Wi-Fi	korkea	1 Mb/s–6.75 Gb/s	20–100 m
Mobiilikommunikaatio	4G:keskitaso	4G:0.1–1 Gb/s	koko kuuluvuusalue
	5G:matala	5G:1-10 Gb/s	
Bluetooth (BLE)	matala	1–24 Mb/s	8–10 m
WSN	korkea	20–250 Kb/s	20–100 m

Taulukko 1. Vertailu teknologioista. Lähteet: Ahmadi ym. 2019; Finkenzeller 2010; Gupta ja Jha 2015

2.2 Langattomat sensoriverkostot ja simulaatiot

Yleisesti monessa tilanteessa olisi hyödyllistä saada tietoa monelta erilaiselta laitteelta, jotka lähettävät ja vastaanottavat erilaista dataa. Näiden yhdistäminen ja niistä hyödyllisten datamallien luonti on yksi haasteista IoT-laitteiden kokonaisvaltaisessa käyttöönotossa. Kokonaisuutta, joka koostuu useasta sensorista, joiden tarkoitus on yhdessä antaa kuva jostakin tilanteesta tai olosuhteista kutsutaan heterogeeniseksi langattomiksi sensovierkoiksi (engl. *Wireless Sensor Network*) (WSN). Tässä sensorit voivat olla mikä tahansa datan lähde teknologiasta tai protokollasta riippumatta (Al-Fagih ym. 2013; Wu ja Chung 2007). Tarve käyttää useaa erilaista sensoria voi kummuta esimerkiksi tarpeesta tutkia useampaa eri attribuuttia, kuten ilmankosteutta ja tuulennopeutta. Voi myös olla, että halutaan yhdistellä halvempia ja kalliimpia sensoreita varojen säästämiseksi tai muuten tarpeen mukaan. WSN-kokonaisuuksista voidaan myös rakentaa simulaatioita määrittämään mikä olisi paras tapa asetella erilaiset sensorit niin että mahdollisimman paljon haluttua tietoa voitaisiin kerätä mahdollisimman vähällä määrällä sensoreita. Al-Fagih ym. (2013) ehdottavat, että Näissä simulaatioissa voidaan WSN:n jakaa neljään osaan: itse sensorit, datan kerääjä, portti ja viimeisenä asiakkaan näkymä datasta. Sensori voi olla vaikka RFID-tunniste, datan ke-

rääjä RFID-skanneri, portti pilvipalvelu ja asiakkaan näkymä puhelinsovellus. Monimutkaisemmissa tilanteissa ja teknologiasta riippuen voidaan soveltaa erilaisia kommunikaatiomalleja. Laitteet voivat olla suoraan yhteydessä toisiinsa, pilvipalveluun tai porttiin (Ahmadi ym. 2019).

2.3 Protokollat

Internetissä on jo toiminnassa monenlaisia tiedonsiirtoprotokollia. IoT-laitteiden näkökulmasta ongelmaksi kuitenkin saattaa muodostua laitteiden pienempi muisti, laskentateho ja verkkoyhteyksien kaistanleveys verrattuna perinteisimpiin internetiin yhdistettyihin laitteisiin. Virrankulutuksen tulisi myös olla mahdollisimman pientä, sillä monet laitteet voivat toimia joko ladattavalla akulla tai paristoilla. Usealle tunnetulle protokollalle, kuten HTTP ja TCP/IP ollaan ehdotettu IoT-laitteiden käyttöön paremmin sopivia versioita. Tästä esimerkkinä ovat coAP ja LoWPAN. coAP (lyhenne engl. sanoista *Constrained application protocol*) on IETF:n (lyhenne engl. sanoista *internet engineering task force*) ehdottama protokolla muuttamaan joitakin HTTP:n ominaisuuksia enemmän esineiden internetille sopivammiksi. LowPAN (lyhenne engl. sanoista *Low-power wireless personal area networks*) lähettää pieniä paketteja, käyttää vähemmän sähköä ja laajakaistaa verrattuna muihin protokolliin. Lisäksi tähän protokollaan ollan kehitetty yhteensopivuus IPv6-internetprotokollan kanssa, missä IPv6:n otsikkokenttää tiivistetään pienemmän paketin koon saavuttamiseksi. Tästä käytetään nimeä 6LoWPAN (Ahmadi ym. 2019).

3 Lääketieteellisten esineiden internet

Lääketieteellisten esineiden internet (engl. *Internet of Healthcare things*) (IoHT) viittaa laitteisiin ja systeemeihin joita voidaan soveltaa lääketieteellisesti, joihin ollaan lisätty IoT-teknologiaa. Joissain lähteissä käytetään myös termiä IoMT (lyhenne engl. sanoista *Internet of Medical things*). Tällaiset sovellukset voivat tarjota vastauksia useampaan suureen haasteeseen terveydenhoidon saralla, kuten esimerkiksi väestön vanhenemiseen, resurssien puutteeseen ja kriisitilanteiden hallitsemiseen (Yin ym. 2016). IoHT-laitteista puhuttaessa voidaan viitata kaikenlaisiin välineisiin joiden katsotaan hoitavan tai monitoroivan ihmisten terveyttä. Tällaisia voisi olla esimerkiksi sydämentahdistin joka lähettää reaaliaikaista tietoa sydämen toiminnasta ja sykkeestä, implantti joka valvoo ja raportoi verensokeriarvoja tai sensori joka pitää kirjaa jossakin tilassa käyneistä ihmisistä tartuntavaaran vuoksi. Muita eri attribuutteja, jotka ovat yleensä mielenkiintoisia terveydehuollon kannalta, ja joita voidaan lähettää verkon yli, ovat esimerkiksi kehon lämpotila, hapenotto, paino, lihassupistukset ja liike (Yin ym. 2016).

Yksi IoHT:n suurista valttikorteista on reaaliaikaisen, tai lähes reaaliaikaisen datan saatavuus. Aika on monen sairauden hoidon tehokkuuden kannalta avainasemassa. Varsinkin hätätapauksissa, hoitoonpääsy ja nopea diagnoosi voivat olla ratkaiseva tekijä potilaan elämän ja kuoleman välillä. Jos sydämentahdistin tai sykemittari havaitse sydäninfarktin ensioireet ja varoittaa niistä etukäteen, on potilaan selviytyminen vähillä vammoilla huomattavasti todennäköisempää. Varsinkin sydäninfarktien oireet voivat vaihdella huomattavasti eri ihmisillä. Monet eivät välttämättä edes tajua mistä heidän oireensa johtuvat. Näissä tapauksissa IoHT-laitteesta olisi suuri apu.

Toinen IoHT-laitteiston mahdollisuuksista on potilaan sairaalassa vietetyn kokonaisajan vähentäminen (Ahmadi ym. 2019). Potilaan tilan seuranta etänä ja tehokas yhteydenpito mahdollistuvat uusien teknologioiden ja niiden käyttöönoton myötä. Tämä olisi hyödyllistä monella eri tapaa. Kummankin potilaan ja sairaalan kustannukset potilaan hoidosta vähenisivät. IoT-laitteilla on ylipäätänsä mahdollisuus kustannusten vähentämiseen niin terveydenhuollossa kuin muussakin liiketoiminnassa, kunhan tarvittava laitteisto on asennettu paikoilleen. Tämä alustava asennus saattaa tosin tuoda alustavan kulujen nousun. Sairaaloissa myös sän-

kypaikat säästyisivät ja sairaalan työntekijöiden aikaa ei kuluisi sellaisten asioiden hoitoon, jotka ovat tehtävissä IoT-laitteiden avulla. Tämä voi myös olla helpotus monelle vaikeasti pitkäaikaissairaalle, sillä vahva etäyhteys terveydenhoitajien kanssa voisi mahdollistaa sen, että heidän ei tarvitsisi vierailla sairaalassa fyysisesti yhtä usein, vaan voisivat evaluoida tilanteensa etänä.

Yleisesti kaikkia hyviä tai huonoja puolia IoHT-laitteistosta ei vielä ennen laajempaa käyttöönottoa osata sanoa. On kuitenkin selvää että IoT voi tehdä sairaanhuollosta monipuolisempaa ja joustavampaa. Se tekisi sairaahuollosta myös kestävämpää ja entistä valmiimpaa erilaisiin poikkeustilanteisiin tarjoamalla monipuolisempia mahdollisuuksia hoitoon, ja erityisesti kotihoitoon (Ahmadi ym. 2019).

IoHT:n piiriin kuitenkin on muodostunut useita haasteita. Monista sensoreista, monenlaisesta datasta ja monista todennusprotokollista muodostuu nopeasti vaikeasti hallittava kokonaisuus (Yin ym. 2016). Toimiva kokonaisuus vaatii tietyn määrän teknistä tietotaitoa systeemin käyttäjiltä. Heidän täytyy osata soveltaa ja päivittää laitteita tarpeen tullen. Tämä käytännössä tarkoittaa sitä että sairaaloiden ja muiden palveluiden, jotka käyttävät IoT:ta tulee sijoittaa varoja henkilöstön kouluttamiseen. Teknologia kehittyy nykypäivänä nopeasti, joten koulutuksen tulee olla myös jatkuvaa.

Kuten mainittua, IoT-laitteiden standardointitaso on heikko. Tämä voi johtaa tilanteisiin missä käytänteet vaihtelevat rajusti, mikä voi tehdä käytöstä ja järjestelmien yhdistämisestä äärimmäisen haasteellista.

Ehdotettu arkkitehtuuristandardi IoHT-laitteille on samankaltainen kuin muillekin IoT-laitteille. Alin kerros on eniten kontaktissa potilaiden tai tutkittavien henkilöiden kanssa. Sen keräämä data välitetään ylemmille kerroksille käsiteltäväksi (Yin ym. 2016). Kuten muissakin IoT-sovelluksissa, pilvipalvelut ja pilvilaskenta ovat merkittävä osa arkkitehtuuria IoHT:ssa (Ahmadi ym. 2019). Pilvilaskenta tarjoaa laskentaa, tallennustilaa ja muita palveluita verkon yli. Tämän etu on se, että IoT- laitteiden pitää vain osata kerätä data ja jollain tapaa välittää se pilvipalvelulle. Muita etuja ovat kustannukset ja palvelun joustavuus. Useat palveluntarjoajat mahdollistavat maksun pelkästään lähetetyn datan perusteella, jolloin asiakas ei maksa mistään muusta kuin käyttämistään palveluista. Toteutus, jonka logiikka sijaitsee jossain

muualla kuin asiakkaan luona on myös testaamisen kannalta hyödyllinen. Eri järjestelmiä voidaan testata ilman että asiakkaan tulisi fyysisesti rakentaa mitään (Stergiou ym. 2018).

4 Lääketieteellisten esineiden internet ja tartuntataudit

Uuden tartuntataudin havaitseminen niin nopeasti kuin mahdollista on elintärkeää. Tähän tarkoitukseen voidaan ehdottaa erilaisia verkkoyhteyksiin perustuvaa valvontaa. Nykyinen kehitys etenkin mobiilitiedonsiirtoteknologiassa mahdollistaa uudenlaisia massiiviseen ja lähes reaaliaikaiseen tiedon keräämiseen perustuvia ratkaisuja (Christaki 2015). IoT tartuntatautien kontekstissa onkin nousussa oleva tutkimusalue (Rahman ym. 2020). Tämän tutkielman kannalta mielenkiintoisia ovat tartuntataudit, jotka leviävät ihmiseltä ihmiselle, pinnalta ihmiselle ja ihmiseltä pinnalle, jos pinta on ollut kontaktissa sairaan ihmisen kanssa. Näin kahdenlaiset teknologiat ovat kiinnostavia: Sellaiset, jotka tarkkailevat jollain tavalla pintoja ja sellaiset, jotka seuraavat ihmisten liikkeitä ja elintoimintoja. Erityisen kiinnostavia ovat myös sellaiset ratkaisut ja mallit, joiden fyysinen infrastruktuuri on jo paikoillaan, esimerkiksi mobiililaitteet, älykellot ja internetyhteydet (Rahman ym. 2020). Yleisesti IoT-teknologia tarjoaa paljon uusia mahdollisuuksia ja innovaatioita tartuntatautien saralla.

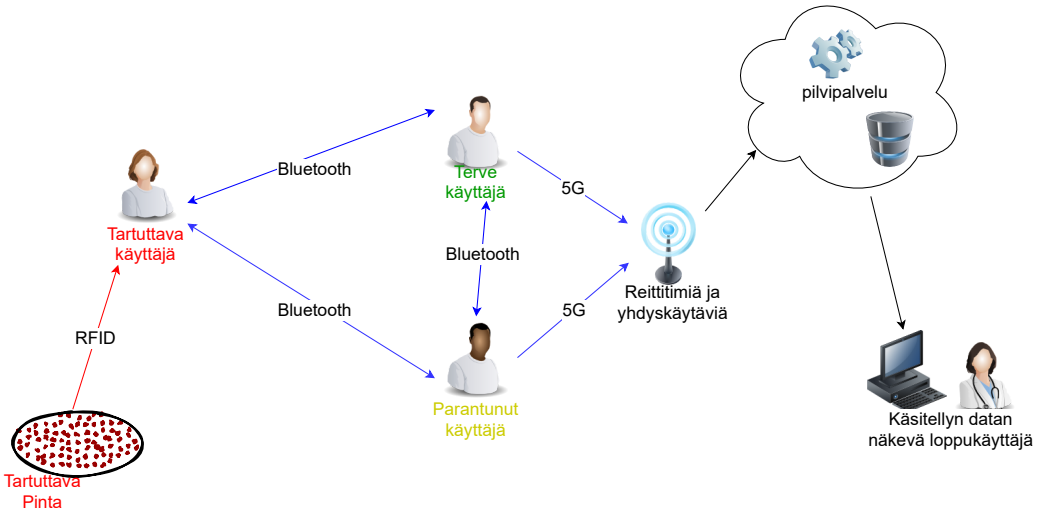
Myös etähoito ja sen kehitys olisi ratkaiseva asia epidemioiden hallitsemisessa, sillä sairaalat ovat tunnetusti ongelmallisia helposti tarttuvien sairauksien kannalta suuren ihmismäärän ja heikossa terveydentilassa olevien potilaiden vuoksi. Jos osa potilaista joiden hoito perinteisesti tapahtuisi sairaalan sisällä pystyttäisiin hoitaa etänä säästyttäisiin mahdollisilta uusilta tartunnoilta ja säästettäisiin resursseja joita voitaisiin tehokkaammin kohdentaa epidemian hoitoon. Tällaisissa etähoidoissa voitaisiin hyödyntää chatbotteja, videosovelluksia ja mobiiliteknologiaa.

COVID-19 pandemia ja sen katastrofaaliset vaikutukset talouteen ja terveydenhuoltoon ovat tuoneet esille tarpeen globaalille tartuntojen valvonta- ja jäljityssysteemeille. IoT-laitteet, joiden teknologinen kehitys ja yleisyys lisääntyy koko ajan voisi tarjota uudenlaisen tavan ennustaa, analysoida, valvoa ja estää tartuntatauteja (Rahman ym. 2020). Tautien puhkeamisen havaitseminen vaatii jatkuvaa suurten ihmismassojen terveydentilan monitorointia pitkällä aikavälillä (Zgheib ym. 2020). Muuta mielenkiintoista tietoa olisi epidemian tila, kuinka monta sairastunutta henkilöä on, missä tartunnat tapahtuvat ja mikä on tartunnan saannin todennäköisyys. Tietoa voitaisiin kerätä laaja-alaisesti heterogeenisista lähteistä. Tämän datan analysointiin käytettäisiin massadatan tutkimisen työkaluja. Massadatasta ja sen ongel-

mista kerrotaan myöhemmin tässä tutkielmassa kappaleessa *Google Flu Trends - varoittava esimerkki*. Ihmisten kulkemisen valvonta ja heidän elintoimintojensa tarkkailu voi myös herättää kysymyksiä yksityisyydenloukkauksista ja muista eettisistä ongelmista joita tartuntatautien ehkäisy mahdollisimman tehokkaalla tavalla saattaa aiheuttaa. Tästäkin kerrotaan enemmän myöhemmin tässä tutkimuksessa kappaleessa *kyberturvallisuus ja lääketieteellisten esineiden internet*.

Valvonta- ja jäljitystekniikoita mietittäessä voidaan tarkastella yleisellä tasolla joko suljettuja tiloja, kuten sairaaloita ja hoitokoteja, tai laajempia alueita jopa globaalilla tasolla. Hieman eri teknologiat korostuvat näissä tilanteissa, ja lähtökohdat ovat hieman erilaiset. Erilaisissa suljetuissa tiloissa tavoite on estää tartunnat kokonaan, kun taas laajemmalla tasolla tavoite on enemmänkin tartuntojen jäljitys. Suljetuissa tiloissa pintojen tarkastelu on suuremmassa roolissa, kun taas ulkomaailmassa ihmisten liikkeet ja läheinen sijainti tosiinsa on tärkeämpää (Hu 2020). Kuitenkin kumpikin tartuntojen esto ja jäljitys on tärkeää kaikissa tapauksissa. Erilaisiin suljettuihin tiloihin voidaan soveltaa laaja-alaisimmin erilaisia laitteita, Onkin syntynyt konsepti älysairaaloista joissa digitaalisen infrastruktuurin käyttö ollaan optimoitu (Guinard 2006). Näin käytännössä jokainen sairaalassa oleva henkilö voidaan yksilöidä RFID-tunnisteella tai muulla sensorilla ja jokainen huone johon hän menee voisi sisältää RFID-lukijan, joka pitää yllä tietokantaa kaikista sen sisällä olevista ihmisistä ja voi hälyttää jos tilassa on liikaa ihmisiä. Erilaisista elintoimintoja mittaavista laitteista voitaisiin saada tietoa lähes reaaliaikaisesti, mikä mahdollistaisi nopean reagoinnin mahdollisiin tartuntoihin (Guinard 2006). Huomattavaa tosin on että digitaaliset tartunnanestotekniikat toimivat yhdessä ei-digitaalisten kanssa, eikävätkä pyri korvaamaan niitä.

Laajemmalla alalla keskitytään jäljittämiseen ja mahdollisten tartuntaketjujen katkaisuun, sairauden maantieteellisen leviämisen valvomiseen ja trendien tunnistamiseen. GPS, Bluetooth, ja langattomat verkkoyhteydet ovat avainteknologioita näissä tapauksissa (Chamola ym. 2020; Hu 2020). Valtiot voivat halutessaan pitää kirjaa henkilöistä jotka voivat mahdollisesti tartuttaa jotakin tautia. GPS:n avulla voidaan jäljittää ihmisten nykyistä sijaintia ja sijainnin historiaa heidän esimerkiksi matkapuhelimistaan ja näin voidaan päätellä missä tartuttavat henkilöt ovat käyneet ja kenet he ovat mahdollisesti altistaneet (Chamola ym. 2020). Bluetooth on yksityisyyttä kunnioittavampi vaihtoehto, sillä se ei jäljitä tarkkaa sijaintia,



Kuvio 1. yksinkertainen IoHT-arkkitehtuuriesimerkki tartuntatautien jäljittämisestä.

vaan läheisyyttä muihin käyttäjiin. Bluetooth-laite etsii lähistöltä muita laitteita, joissa on jäljitys käynnissä ja pitää kirjaa niistä. Jos jos jokin käyttäjä osoittautuu tartuttajaksi, voidaan siitä ilmoittaa kaikille hänen läheisyydessään olleille. Bluetoothin huono puoli on juuri se, että ilman tarkkaa sijaintia ei voida päätellä mahdollisesti tartuttavien henkilöiden liikkumista esimerkiksi julkisilla paikoilla (Chamola ym. 2020; Hu 2020).

Muistakin jokapäiväisistä laitteista voidaan kerätä dataa liittyen epidemioihin IoT-periaatteiden mukaisesti. Esimerkiksi internetiin yhteydessä olevat kuumemittarit joita ollaan jaettu tietyille alueille voivat kertoa mahdollisista kuumetautien leviämisestä alueilla (Chamola ym. 2020). Älykellot ja muu puettava teknologia voi havaita poikkeamia sykkeessä, aktiivisuudessa ja veren happipitoisuudessa indikoiden sairautta. Kuitenkin mitä enemmän eri datalähteitä otetaan mukaan terveysdatan tutkimukseen, sitä haastavampaa sen analysoimisesta tulee (Al-Fagih ym. 2013; Zgheib ym. 2020). Tästä seuraa skaalautuvuusongelma. Kun dataa analysoidaan niin että ihmisten jokapäiväisistä aktiviteeteistä (engl. *activities of daily life*) (ADL) kerättystä datasta yritetään tunnistaa sairauksiin sopivia malleja (engl. *the epidemic model*), jokaisessa analyysiprosessin askeleessa laskennan kompleksisuus nousee (Zgheib ym. 2020). Datan määrän kasvaessa siis laskennan määrä saattaa nousta niin korkeaksi, että sitä ei pystytä käsittelemään. Lisää tutkimusta tarvitaan paremmin skaalautuvista ratkaisuista. Tulevaisuuden tutkimuksessa on tärkeää työskennellä yhdessä terveysalan ammattilaisten kanssa,

jotta tuloksista saadaan mahdollisimman oikeellisia ja käytännöllisiä.

5 Google Flu Trends – varoittava esimerkki

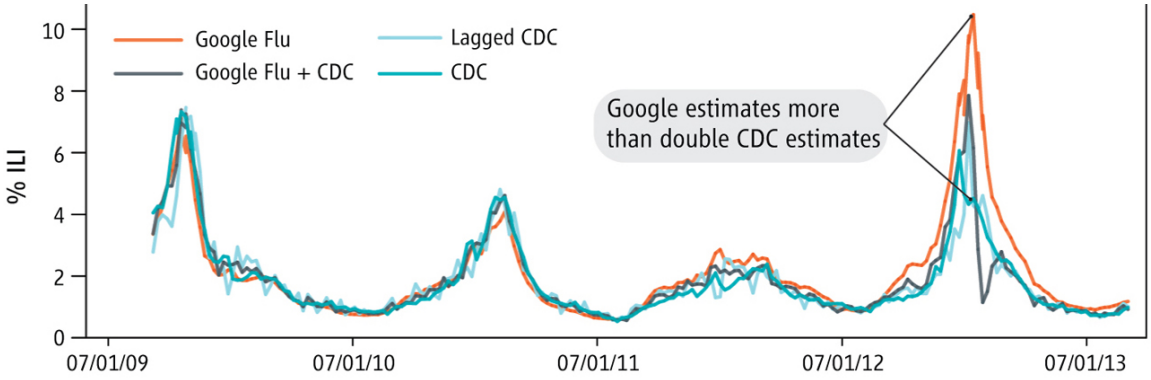
Google flu trends (GFT) oli projekti joka kehitettiin generoimaan reaaliaikaisia ennustuksia nuhakuumeen kaltaisten tartuntatautien (engl. *Influenza Like Illness*, ILI) leviämisestä louhimalla dataa Googlen hakukoneen hakulauseista ja suosiota ennakoivista algoritmeista (Santillana ym. 2014). Projekti oli aktiivinen vuosina 2008-2015. Datan louhinta perustui siihen, että jos jollain alueilla haettiin flunssan oireita enemmän kuin normaalisti, oletetaan että alueella on piikki flunssatapauksissa. Luonnollisesti projekti generoi valtavia määriä analysoitavaa dataa. Arvioitiin että näin saatasiin tietoa flunssakausista ja ongelma-alueista nopeammin kuin perinteisimmillä menetelmillä (Butler 2013).

Kuitenkin jo vuonna 2009 kävi ilmi, että GFT:n ennustukset eivät ole tarpeeksi tarkkoja. GFT aliarvioi vuoden 2009 H1N1-pandemian sairastuneiden määrän (Butler 2013) ja pahimmillaan yli tuplasti yliarvioi vuosien 2012-2013 yhdysvaltain influenssakauden tartuntapiikin. (Lazer ym. 2014). Huomattavaa on että H1N1-pandemia tapahtui influenssakauden ulkopuolella.

Mikä sitten meni pieleen? Ongelmaksi muodostui massadatan (engl. big data) käsittelyssä yleinen ongelma nimeltään ylisovitus (engl. overfitting) (Lazer ym. 2014; Lampos ym. 2015). Datan laadun ja määrän takia ei osata tarkasti muodostaa oikeanlaisia malleja datapisteistä. GFT:n ongelmaksi muodostui muut kausiluontoiset hakukoneiden haut, joiden relevanssi nousee samaan aikaan kausiflunssan kanssa, mutta jolla ei todellisuudessa ole mitään tekemistä sen kanssa. Esimerkiksi käärmeenpureman oireista tiedon hakeminen on kausiluontoinen ilmiö, mutta ei omalta osaltaan liity mitenkään influenssatilanteeseen (Lazer ym. 2014). Näin GFT:n algoritimi ennusti kausiluontoiset sairastumisluvut suuremmiksi kuin ne todellisuudessa olivat. Tämä ilmiö esiintyi käänteisenä H1N1-pandemian aikaan, kun GFT:n algoritmi ei osannut odottaa influenssakauden ulkopuolella tapahtuvaa nuhakuumeen puhkeamista, koska kausiflunssan kanssa samanaikaiset hakukoneiden haut puuttuivat. Siksi sairastuneiden määrä aliarvioitiin (Santillana ym. 2014; Lazer ym. 2014).

Tämä tuo esille erään digitaalisen tautientunnistuksen ongelman. Kaikki toiminta, vaikka se viittaisikin sairauteen, ei välttämättä ole sitä. Jotkin yhdistävät tekijät voivat vahvasti korre-

loida sairauden puhkeamisen kanssa, mutta todellisuudessa näin ei ole. Korrelaatio ei implikoi kausaliteettia. Tämä voi osoittautua suureksi haasteeksi esimerkiksi koneoppimisalgoritmien kanssa jotka analysoivat terveysdataa. Toinen huomattava ongelma oli Googlen haluttomuus olla läpinäkyvä GFT:n käyttämien algoritmien kanssa - tehottomille algoritmeille ei voida ehdottaa ratkaisua, jos niiden toiminta ei ole tiedossa.



Kuvio 2. visualisaatio GFT:n epäonnistumisesta. CDC on virallinen yhdysvaltain tautikeskus. “Lagged CDC” sisältää 52 viikon kausivaihtelumuuttujat ja viiveelliset(2-viikkoa vanhat) CDC-tiedot. "Google Flu + CDC"yhdistää GFT: n, viiveelliset CDC-estimaatit ja viivästyneen virheen GFT-arvioissa. lähde: (Lazer ym. 2014).

GFT:n ongelmille ei löydy yhtä yleispätevää ratkaisua, mutta parannuskeinoja ollaan ehdotettu vertailemalla virallisia flunssatilastoja ja GFT:n ennukstuksia. Ylipäätänsä massadatan käyttö lääketieteellisessä kontekstissa vaatii lisää tieteellistä tutkimusta. Kuvio 2 osoittaa, että yhdistelemällä erilaisten virallisten tahojen perinteisesti yleensä laboratorioraporttien mukaan tehtyjä estimaatteja influenssankaltaisten tautien leviämisestä, saadaan hyvinkin tarkkoja arvioita tilainteista. GFT:n dataa ja CDC:n 2-viikkoa vanhaa dataa prjektoimalla saadaan tarkempi arvio, kuin pelkää GFT:n dataa tarkastelemalla (Lazer ym. 2014).

6 Kyberturvallisuus ja lääketieteellisten esineiden internet

Terveyteen liittyvä data luokitellaan äärimmäisen herkkäluontoiseksi dataksi. Tietoturvan kannalta, myös dataan saisi päästä käsiksi vain sellaiset henkilöt, joilla on oikeus siihen tai joiden työn kannalta se on relevanttia (“Health data in the workplace” 2021).

Valitettavasti maailmanlaajuista standardia IoT-laitteiden tietoturvan tarkasteluun ei ole. Kuitenkin fiksuja ratkaisuja voidaan tarkastella. Ensinnäkin teknisellä tasolla laitteiden kommunikaation pitäisi olla päittäin salatuttua (engl. *end-to-end encryption*) (E2EE), koska kyse on nimenomaan terveyteen liittyvästä datasta (Strielkina ym. 2018). Tämä tarkoittaa sitä että viestiliikennettä IoT-laitteen ja sen vastaanottajan välillä ei välitetä salaamatta kolmannen osapuolen kautta, kuka voisi päästä siihen käsiksi ja mahdollisesti myydä sitä etenpäin tai muutoin väärinkäyttää. Lähettäjä salaa datan ja vain vastaanottaja osaa purkaa sen.

IoT-laitteiden dataliikenteen vaarantuminen voidaan jakaa karkeasti kahteen osaan: tahalliset uhat ja tahattomat uhat. Tahattomiin uhkiin kuuluu sellaiset uhat, jotka tapahtuvat vahingossa tai tarkoituksettomasti. Uhka voi liittyä monimutkaiseen IT-infrastruktuuriin ja sen toimintahäiriöihin (Strielkina ym. 2018). Tällaisia ovat esimerkiksi laitehäiriöt, verkkoyhteyshäiriöt tai ohjelmistobugit.

Tahalliset uhkat ovat sellaisia missä hyökkääjä yrittää tahallisesti päästä käsiksi dataan jotakin kautta. IoT pohjaiset systeemit tyypillisesti sisältävät kolme haavoittuvaista kohtaa: itse laite, kommunikaatiolinkki ja vastaanottajapalvelin (Omoogun ym. 2017). Tällasia uhkia ovat esimerkiksi palvelunestohyökkäykset palvelimille (engl. *Denial of Service*) (DoS), datan salakuuntelu kun sitä lähetetään (engl. *Man In The Middle*) (MITM) tai identiteetin huijaus (engl. *identity spoofing*), jossa väärä henkilö käyttää sensoreita sekoittaen analysoitavan datan (Omoogun ym. 2017). Tahallisiin uhkiin liittyy paljon teoreettisia uhkia joita ei oikeastaan ole koskaan tapahtunut, mutta joiden toteutuminen on mahdollista.

Yhdysvaltain sisäisen turvallisuuden ministeriö tekee tutkimusta useasta lääketieteellisestä laitteesta, joissa on mahdollisia haavoittuvuuksia. Tällaiset haavoittuvuudet voisivat pahimmassa tapauksessa aiheuttaa potilaan kuoleman. Teoriassa olisi mahdollista ohjelmistohaavoittuvuuksia hyväksikäyttämällä hakkeroida sydänimplantti niin, että se aiheuttaa tappavan

sähköiskun käyttäjälleen tai käskemään infuusiopumpun yliannostamaan potilaan lääkitys (“U.S. government probes medical devices for possible cyber flaws” 2014).

7 Etiikkaa

Kaikkia eettisiä ongelmia, mitä laaja IoHT-tekniikan käyttöönotto tuo tullessaan ei vielä tunneta, mutta mahdollisia ongelmakohtia voidaan silti eritellä. Eettisiä ongelmia voi olla esimerkiksi:

- Miten taata datan turvallisuus ja yksityisyys?
- Äärimmäisen herkkäluonteinen data ja sen analysointiin liittyvät haasteet.
- Kuka omistaa datan? Henkilö josta se kerättiin voiko datan kerääjät?
- Miten torjua mahdollista laitteista aiheutuvaa stigmaa?

Uudet teknologiat mahdollistavat sen, että esineet ja asiat jotka ovat perinteisesti olleet osa yksityistä elämää voivat mahdollisesti lähettää tietoa, jota pääsee tutkimaan potentiaalisesti suuri määrä vieraita ihmisiä. Tämä luonnollisesti herättää kysymyksen, kuinka paljon omaa yksityisyyttänsä ihmiset olisivat valmiita uhraamaan sen eteen että he saisivat käyttöönsä IoT-laitteita ja kuinka paljon yksityisyyttä voidaan loukata tehokkaamman hoidon puolesta (Mittelstadt 2017). Yleisesti voidaan päätellä, että IoT-laitteisiin kuuluu kiinteällä tavalla kompromissi turvallisuuden ja yksityisyyden välillä (Mittelstadt 2017). Tästä syystä IoT-laitteisto terveydenhuollossa tulee rakentaa käyttäjien yksityisyyttä mahdollisimman paljon kunnioittaen.

Jotta potilas pystyy tekemään päätöksen laitteen käyttöönotosta osana hoitoa, täytyy hänen olla tietoinen sen toiminnasta (Bowes, Dawson ja Bell 2012). Tämä vaatii sen, että ensinnäkin potilaan täytyy tietää miten hänen hoitonsa toimii ja miten hänen dataansa kerätään ja kuinka se analysoidaan. Dataa ei saa käyttää mihinkään tarkoitukseen, johon potilas ei ole erityisesti antanut lupaa. Ongelmaksi muodostuu, miten monimutkaisista prosesseista kerrotaan potilaille, jotka voivat olla tietämättömiä perustavanlaatuisistakin teknologioista. Tyypillisesti tällaisia ihmisryhmiä ovat vanhukset ja muut henkilöt joilla on alentunut kognitiivinen toimintakyky (Bowes, Dawson ja Bell 2012). Voidaan pohtia, missä menee raja yksityisyyden loukkaamisen ja tarpeellisen hoidon välillä jos potilas ei tiedä mitä tietoa hänestä kerätään ja milloin. Potilas voi myös unohtaa että hänen käyttämät laitteensa ovat yhteydessä verkkoon, mikä luo tilanteen jossa datan keräämisen jatkaminen ja luvallisuus on

kyseenalaista.

Heikossa asemassa olevien ihmisten kanssa työskennellessä ihmissuhteet ja niiden tärkeys korostuvat. Tutkimukset ovat osoittaneet että varsinkin vanhukset pelkäävät IoT-laitteiston korvaavan heidän sosiaalisen kanssakäymisen hoitajien kanssa (Mittelstadt 2017). Sosiaalisuus ja ihmissuhteet ovat tärkeitä ihmisille. IoHT ei saa aiheuttaa eristäytymistä ja yksinäisyyttä, vaan ihmissuhteiden ylläpito pitää olla mukana hoitosuunnitelmassa.

Laitteiden näkyvyys niitä käytettäessä vaikuttaa niiden pitkäaikaiskäyttöön ja voi aiheuttaa stigmaa muiden ihmisten keskuudessa (Mittelstadt 2017). IoT-laitteet voivat aiheuttaa stigmaa, varsinkin jos ne ovat puettavia ja näkyviä (Courtney 2008). Näissä tapauksissa latteiden käytettävyys kärsii ja hoito voi aiheuttaa sosiaalista painetta potilaalle. Esimerkkinä voidaan tarkastella tilannetta joissa jostakin tarttuvasta taudista parantuvia ihmisiä hoidetaan puettavalla IoT-laitteilla, vaikka potilas ei enään tartuttaisi ketään, laite saattaa aiheuttaa irrationaalista stigmaa ja pelkoa muissa ihmisissä. Laitteen tulisi siis olla mahdollisimman huomaamaton tai yleinen, kuten kello tai puhelin. Tällaisilla laitteilla on vähemmän taipumusta aiheuttaa negatiivisia reaktioita ja stigmaa (Mittelstadt 2017).

8 Yhteenveto ja johtopäätökset

Tutkimuksessa ollaan tarkasteltu IoT-teknologiaa yleisesti, terveydenhoidon näkökulmasta ja lopulta tartuntatautien hoidon kannalta. Myös erinäisiä ongelmakohtia liittyen massadataan, kyberturvallisuuteen ja etiikkaan ollaan käsitelty.

IoT tarjoaa lupaavia ratkaisuja, jolla mahdollisuus ratkaista monia ongelmia erityisesti tartuntatautien kannalta, mutta myös sairaalahoidossa joustavan hoidon ja resurssipulan kannalta. Kuitenkin IoT-systeemeissä on pahoja aukkoja turvallisuudessa, standardeissa ja skaalautuvuudessa. Pahimmassa tapauksessa tämä saattaa johtaa tilanteeseen, jossa IoT:n huonot puolet kumoavat hyvät puolet ja potilaiden turvallisuus ja yksityisyys kärsii. IoT luokin tilanteen, jossa tasapainotellaan uhkien ja hyötyjen välillä. Ainakin tällä hetkellä tulee päätös laitteiden käyttöönotosta tehdä tapauskohtaisesti, laitteiden käyttäjien tulee olla informoituja teknologiasta ja heillä tulee olla sananvaltaa laitteiden käytöstä.

Tulevaisuuden tutkimuksissa ei tulisikaan niinkään enään kartoittaa sitä, mitä kaikkea pystytään toteuttaa IoT-laitteilla terveydenhuollossa, vaan mikä on pakollista ottaa huomioon, jotta niiden myynti ja käyttöönotto olisi mahdollista ja kannattavaa niin kehittäjille kuin lääketieteen ammattilaisillekin (Mani ja Chouk 2018). On tyypillistä, että kun perinteisiä menetelmiä korvataan jollakin uudella teknologialla, syntyy resistanssia käyttäjien keskuudessa. Tämä johtuu monista syistä. Terveydenhuollon kannalta relevanteimmat ovat oletettu laitteiden vaikeakäyttöisyys, oletetut tietoturvallisuusriskit ja oletetut negatiiviset vaikutukset terveyteen (Kim ja Kim 2018). Näiden vuoksi on äärimmäisen tärkeää luoda selkokielinen yhteys tietotekniikan ammattilaisten ja laitteita jokapäiväisessä elämässään käyttävien henkilöiden välille, olivat he sitten terveydehuollon ammattilaisia tai potilaita.

Lisää tutkimusta siis standardeista, käytettävyydestä ja niiden puitteiden luomisesta tarvitaan, koska niiden pohjalta voi hyvin lähteä muotoilemaan vastauksia muihin ongelmiin IoT:n käyttöönotossa. Esimerkiksi kyberturvallisuutta on paljon helpompaa kehittää, jos tiedetään miten laitteet yleisesti toimivat.

Lähteet

"about bluetooth". 2021. https://www.bluetooth.com/about-us/.

Ahmadi, Hossein, Goli Arji, Leila Shahmoradi, Reza Safdari, Mehrbakhsh Nilashi ja Mojtaba Alizadeh. 2019. "The application of internet of things in healthcare: a systematic literature review and classification". *Universal Access in the Information Society* 18 (4): 837–869.

Bowes, Alison, Alison Dawson ja David Bell. 2012. "Ethical implications of lifestyle monitoring data in ageing research". *Information, Communication & Society* 15 (1): 5–22.

Butler, Declan. 2013. "When Google got flu wrong". *Nature News* 494 (7436): 155.

Cerf, V., ja R. Kahn. 1974. "A Protocol for Packet Network Intercommunication". *IEEE Transactions on Communications* 22 (5): 637–648. https://doi.org/10.1109/TCOM.1974.1092259.

Chamola, Vinay, Vikas Hassija, Vatsal Gupta ja Mohsen Guizani. 2020. "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact". *Ieee access* 8:90225–90265.

Chang, Kuor-Hsin. 2014. "Bluetooth: a viable solution for IoT?[Industry Perspectives]". *IEEE Wireless Communications* 21 (6): 6–7.

Christaki, Eirini. 2015. "New technologies in predicting, preventing and controlling emerging infectious diseases". *Virulence* 6 (6): 558–565.

Courtney, Karen L. 2008. "Privacy and senior willingness to adopt smart home information technology in residential care facilities".

Eckhardt, Manon, Judd F Hultquist, Robyn M Kaake, Ruth Hüttenhain ja Nevan J Krogan. 2020. "A systems approach to infectious disease". *Nature Reviews Genetics* 21 (6): 339–354.

Al-Fagih, Ashraf E, Fadi M Al-Turjman, Waleed M Alsalih ja Hossam S Hassanein. 2013. "A priced public sensing framework for heterogeneous IoT architectures". *IEEE Transactions on Emerging Topics in Computing* 1 (1): 133–147.

Finkenzeller, Klaus. 2010. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication.* John wiley & sons.

Guinard, Patrik Fuhrer Dominique. 2006. "Building a smart hospital using RFID technologies". Teoksessa *European Conference on eHealth 2006,* toimittanut Henrik Stormer, Andreas Meier ja Michael Schumacher, 131–142. Bonn: Gesellschaft für Informatik e.V.

Gupta, Akhil, ja Rakesh Kumar Jha. 2015. "A survey of 5G network: Architecture and emerging technologies". *IEEE access* 3:1206–1232.

"Health data in the workplace". 2021. Viitattu 2. huhtikuuta 2021. https://edps.europa.eu/data-protection/data-protection/reference-library/health-data-workplace_en.

Hu, Peng. 2020. "IoT-based Contact Tracing Systems for Infectious Diseases: Architecture and Analysis". *arXiv preprint arXiv:2009.01902.*

Kaplan, Elliott, ja Christopher Hegarty. 2005. *Understanding GPS: principles and applications.* Artech house.

Kim, Suwon, ja Seongcheol Kim. 2018. "User preference for an IoT healthcare application for lifestyle disease management". *Telecommunications Policy* 42 (4): 304–314.

Lampos, Vasileios, Andrew C Miller, Steve Crossan ja Christian Stefansen. 2015. "Advances in nowcasting influenza-like illness rates using search query logs". *Scientific reports* 5 (1): 1–10.

Lazer, David, Ryan Kennedy, Gary King ja Alessandro Vespignani. 2014. "The parable of Google Flu: traps in big data analysis". *Science* 343 (6176): 1203–1205.

Li, Shancang, ja Li Da Xu. 2017. *Securing the internet of things.* Syngress.

Lu, Yang, ja Li Da Xu. 2018. "Internet of Things (IoT) cybersecurity research: A review of current research topics". *IEEE Internet of Things Journal* 6 (2): 2103–2115.

Madakam, Somayya, Vihar Lake, Vihar Lake, Vihar Lake ym. 2015. "Internet of Things (IoT): A literature review". *Journal of Computer and Communications* 3 (05): 164.

Mani, Zied, ja Inès Chouk. 2018. “Consumer resistance to innovation in services: challenges and barriers in the internet of things era”. *Journal of Product Innovation Management* 35 (5): 780–807.

Mittelstadt, Brent. 2017. “Ethics of the health-related internet of things: a narrative review”. *Ethics and Information Technology* 19 (3): 157–175.

Omoogun, Michelle, Preetila Seeam, Visham Ramsurrun, Xavier Bellekens ja Amar Seeam. 2017. “When eHealth meets the internet of things: Pervasive security and privacy challenges”. Teoksessa *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security),* 1–7. IEEE.

Rahman, Md Siddikur, Noah C Peeri, Nistha Shrestha, Rafdzah Zaki, Ubydul Haque ja Siti Hafizah Ab Hamid. 2020. “Defending against the Novel Coronavirus (COVID-19) outbreak: How can the Internet of Things (IoT) help to save the world?” *Health policy and technology.*

Rahmani, Amir M, Tuan Nguyen Gia, Behailu Negash, Arman Anzanpour, Iman Azimi, Mingzhe Jiang ja Pasi Liljeberg. 2018. “Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach”. *Future Generation Computer Systems* 78:641–658.

Santillana, Mauricio, D Wendong Zhang, Benjamin M Althouse ja John W Ayers. 2014. “What can digital disease detection learn from (an external revision to) Google Flu Trends?” *American journal of preventive medicine* 47 (3): 341–347.

Selvaraj, Sureshkumar, ja Suresh Sundaravaradhan. 2020. “Challenges and opportunities in IoT healthcare systems: a systematic review”. *SN Applied Sciences* 2 (1): 1–8.

Stergiou, Christos, Kostas E Psannis, Byung-Gyu Kim ja Brij Gupta. 2018. “Secure integration of IoT and cloud computing”. *Future Generation Computer Systems* 78:964–975.

Strielkina, Anastasiia, Oleg Illiashenko, Marina Zhydenko ja Dmytro Uzun. 2018. “Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment”. Teoksessa *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT),* 67–73. IEEE.

"U.S. government probes medical devices for possible cyber flaws". 2014. Viitattu 2. huhtikuuta 2021. https://www.reuters.com/article/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.

Wu, Chun-Hsien, ja Yeh-Ching Chung. 2007. "Heterogeneous Wireless Sensor Network Deployment and Topology Control Based on Irregular Sensor Model". Teoksessa *Advances in Grid and Pervasive Computing,* toimittanut Christophe Cérin ja Kuan-Ching Li, 78–88. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-72360-8.

Yin, Yuehong, Yan Zeng, Xing Chen ja Yuanjie Fan. 2016. "The internet of things in healthcare: An overview". *Journal of Industrial Information Integration* 1:3–13. ISSN: 2452-414X. https://doi.org/https://doi.org/10.1016/j.jii.2016.03.004.

Zgheib, Rita, Stein Kristiansen, Emmanuel Conchon, Thomas Plageman, Vera Goebel ja Rémi Bastide. 2020. "A scalable semantic framework for IoT healthcare applications". *Journal of Ambient Intelligence and Humanized Computing,* 1–19.