Paula Kotilainen

Puettavien älylaitteiden tietoturvariskit

Scoping kirjallisuuskatsaus

Metropolia Ammattikorkeakoulu

Kliinisen asiantuntijuuden tutkinto-ohjelma sosiaali- ja terveysalalla

Ylempi AMK-tutkinto

Digitaalisten palvelujen asiantuntija

Opinnäytetyö 2.5.2024

Tiivistelmä

Tekijä(t):	Paula Kotilainen
Otsikko:	Puettavien älylaitteiden tietoturvariskit
Sivumäärä:	68 sivua + 2 liitettä
Aika:	2.5.2024
Tutkinto:	Sairaanhoitaja (YAMK)
Tutkinto-ohjelma:	Kliininen asiantuntija, sosiaali- ja terveysala
Suuntautumisvaihtoehto:	Digitaalisten palvelujen asiantuntija
Ohjaaja(t):	Yliopettaja Anu Valtonen

Terveydenhuoltoala on viime vuosina ottanut merkittäviä kehitysaskeleita ja puettavat älylaitteet tekevät tuloaan osaksi digitaalista terveydenhuoltoa. Opinnäytetyön tarkoituksena on selvittää, mitä tietoturvariskejä puettavat älylaitteet sisältävät ja kuinka ne vaikuttavat käyttäjien tietosuojaan. Työ pyrkii tuottamaan kattavan ja ajantasaisen katsauksen aiheesta.

Työ toteutettiin scoping katsauksena ja tiedonhaku suoritettiin ennalta määriteltyjen hakulausekkeiden avulla Cinahl-, IEEEXplore-, ProQuest Central- ja PubMed-tietokannoista sekä manuaalisesti Google Scholarista. Aineistoksi valittiin kahdeksantoista vertaisarvioitua artikkelia, jotka vastasivat sisäänotto- ja poissulkukriteereihin. Aineistolle tehtiin laadunarvio JBI arviointikriteeristöllä, aineisto analysoitiin teemoittelun avulla.

Tulokset osoittavat, että puettavien älylaitteiden tietoturvariskit ovat moninaisia ja ulottuvat laajasti yksityisyyden ja tietosuojan loukkauksista haavoittuvuuksiin ja turvallisuusuhkiin. Laitteiden kykyyn seurata käyttäjiä ja heidän toimintaansa jatkuvasti sekä kerätä arkaluontoisia tietoja ilman selkeää suostumusta liittyy riskejä, erityisesti laitteiden IoT-verkkoihin integroinnin myötä. Älysovellusten pyytämät laajat käyttöoikeudet ja sensoridatan käsittely tuovat esiin henkilökohtaisia tietoja ilman käyttäjien aktiivista tietoisuutta siitä, miten tietoja käytetään tai myydään kaupallisiin tarkoituksiin. Tämä asettaa GDPR:n vaatimustenmukaisuuden kyseenalaiseksi. Haasteita ilmenee myös tietoturvan teknisessä toteutuksessa, sillä puettavien laitteiden suunnittelu ja valmistus eivät täytä tietoturvan vaatimuksia. Tulokset korostavat tarvetta päivittää lainsäädäntöä ja standardeja, jotta ne pysyisivät ajan tasalla nopeasti kehittyvän teknologian kanssa ja takaisivat puettavien laitteiden turvallisen käytön.

Johtopäätöksenä voidaan todeta, että puettavien älylaitteiden tietoturvariskien monimuotoisuus ja vaikutus käyttäjien tietosuojaan vaativat tarkkaa huomiota ja jatkuvaa päivitystä tietoturvakäytäntöihin sekä käyttäjien tietoisuuden lisäämistä. Tietosuojan ja käyttäjien oikeuksien turvaaminen edellyttää lainsäädännön, standardien sekä valmistusprosessien ajantasaista kehittämistä. Tulevan EU:n radiolaitedirektiivin vaikutuksia puettavien älylaitteiden tietoturvaan olisi syytä tarkastella jatkossa.

Avainsanat:
Puettavat älylaitteet, wearable, tietoturvariski, yksityisyyden hallinta

Abstract

Author(s):	Paula Kotilainen
Title:	The security risks of wearable smart devices
Number of Pages:	68 pages + 2 appendices
Date:	2 May 2024
Degree:	Master of Health Care (Nursing)
Degree Programme:	Master´s Degree Programme in Clinical Expertise in Health Care and Social Services
Specialisation option:	Expertise in Digital Social and Health Services
Instructor:	Anu Valtonen Principal Lecturer

The healthcare sector has taken significant steps forward in recent years, and wearable smart devices are making their way into digital healthcare. The aim of this master's thesis was to explore the security risks of wearable smart devices and how they affected users' privacy. It aimed to provide a comprehensive and up-to-date overview of the topic.

The work was carried out as a scoping review, and data was searched using predefined search terms from Cinahl, IEEEXplore, ProQuest Central and PubMed databases and manually from Google Scholar. Eighteen peer-reviewed articles that met the inclusion and exclusion criteria were selected. The data were quality assessed using the JBI assessment criteria and analysed using the methods of thematic analysis.

The findings of the master's thesis showed that the security risks of wearable smart devices were diverse, ranging from privacy and data breaches to vulnerabilities and security threats. The ability of wearable devices to continuously monitor users and their activities and collect sensitive data without explicit consent posed risks, especially when devices were integrated into IoT networks. The extensive permissions required by smart applications and the processing of sensor data revealed personal information without the user's active awareness of how the data would be used or sold for commercial purposes. This called into question with the GDPR compliance. The challenges were not limited to data protection, but also to the technical implementation of data security, where the design and manufacturing of wearable devices did not meet data security requirements. The findings highlighted the need to update legislation and standards to keep pace with rapidly evolving technologies, and to ensure the secure use of wearable devices.

In conclusion, the complexity of the security risks posed by wearable smart devices and the impact on users' privacy require careful attention and continuous updating of security policies and user awareness. The protection of privacy and user rights requires the ongoing development of legislation, standards and manufacturing processes. The impact of the forthcoming EU Radio Equipment Directive on the security of wearable smart devices should be further explored.

Keywords:
wearable, wearable smart device, security risk, privacy

Sisällys

1 Johdanto

Puettavien älylaitteiden suosio on kasvanut viime vuosina. Laitteita ovat esimerkiksi älykellot, älyrannekkeet ja älyvaatteet. Ne tarjoavat monia hyödyllisiä toimintoja, kuten terveyden seurantaa, liikuntatietojen tallennusta ja viestintämahdollisuuksia. Kuitenkin puettavissa älylaitteissa piilee myös merkittäviä tietoturvariskejä, jotka voivat vaarantaa käyttäjien yksityisyyden ja tietosuojan. Tämän vuoksi on tärkeää ymmärtää riskien olemassaolo sekä kuinka niitä voidaan hallita. (Holstcentrewebinars.com 2020.) Ficomin mukaan esimerkiksi älykellojen toimitukset kasvavat yli 10 % vuodessa ollen 2021 vuonna 229,5 miljoonaa laitetta. Tämä korostaa, että tietoturvaongelma ei ole mitätön, vaan se on otettava vakavasti. (Ficom.fi.)

Terveydenhuoltoala on viime vuosina ottanut merkittäviä askeleita kohti digitaalista terveydenhuoltoa ja puettavat älylaitteet ovat olleet keskeisessä roolissa tässä kehityksessä. Älylaitteet mahdollistavat potilaiden terveyden ja hyvinvoinnin seurannan reaaliajassa ja voivat auttaa havaitsemaan terveysongelmia varhaisessa vaiheessa. Tämä on erityisen tärkeää väestön ikääntyessä ja terveydenhuollon resurssien ollessa rajalliset. (Handolin & Hämäläinen 2022.) Siksi jokaisen, joka työskentelee sosiaali- ja terveysalalla, tulisi hallita ainakin perustiedot puettavien älylaitteiden tietoturvasta. Terveydenhuollon ammattilaiset saattavat kohdata potilaita, jotka käyttävät laitteita ja heidän on kyettävä tarjoamaan ohjeita niiden turvalliseen käyttöön. Lisäksi terveydenhuollon alalla noudatetaan tiukkaa lainsäädäntöä potilaiden tietosuojasta, mikä korostaa tarvetta ymmärtää laitteiden tietoturvariskit. (Kettunen ym. 2020: 36.)

Puettavissa älylaitteissa hyödynnetään elektronista tekniikkaa tiedon keräämiseen ja jakamiseen reaaliaikaisesti. Laitteet tallentavat liiketietoja päivittäisestä toiminnasta ja synkronoivat ne mobiililaitteiden tai kannettavien tietokoneiden kanssa. Yllättävää kyllä, puettavien älylaitteiden tietoturvaan ei kiinnitetä yhtä paljon huomiota kuin muihin tietoteknisiin ratkaisuihin. Tämä on huolestuttavaa, sillä laitteiden käyttö kasvaa nopeasti, mutta tietoturva ja lainsäädäntö eivät aina pysy kehityksen vauhdissa. Esineiden internet (Internet of things, josta käytetään tässä opinnäyteyössä lyhennettä IoT) luo omat haasteensa tietoturvalle, kun laitteet kommunikoivat keskenään ilman ihmisen väliintuloa. (Weber 2015: 619.) On myös merkittävää, että laki kieltää tunnistettavien henkilötietojen keräämisen, mutta IoT:ssä tämä sääntö voidaan kiertää sillä perusteella, että tiedot eivät liity suoraan tiettyyn henkilöön, vaikka ne olisivatkin

henkilökohtaisia. Kaikki nämä tekijät tekevät tietoturvariskien tunnistamisesta ja hallinnasta erityisen haasteellista. (Ahlmeyer & Chircu 2016: 22–23.)

Opinnäytetyön tarkoituksena on selvittää, mitä tietoturvariskejä puettavat älylaitteet sisältävät ja tunnistaa tekijät, jotka vaikuttavat näiden laitteiden tietoturvariskeihin. Opinnäytetyö pyrkii tuottamaan kattavan ja ajantasaisen katsauksen aiheesta. Tavoitteena on lisätä käyttäjien, valmistajien ja muiden sidosryhmien tietoisuutta puettavien älylaitteiden tietoturvariskeistä ja niiden merkityksestä käyttäjälle. Opinnäytetyön tuloksia voivat hyödyntää kaikki terveydenhuollon toimijat, laitteiden valmistajat ja tutkijat, jotka osallistuvat digitaalisen terveydenhuollon kehittämiseen ja käyttöön.

2 Puettavat älylaitteet

2.1 Historia

Puettavien älylaitteiden historian katsotaan alkaneen lähteestä riippuen tietokoneiden aikakaudelta 1950-luvulta aina silmälasien keksimiseen jo 800 vuotta sitten. Älylaitteella tarkoitetaan nykypäivänä laitetta, jossa on vähintäänkin siru tietojen tallentamiseen mutta historiaa tarkastellessa älylaite on ollut käyttäjälle parempaa kokemusta tarjoava laite. Tästä esimerkkinä ensimmäinen tunnettu versio älysormuksesta, joka oli Abacus-rengas Qing-dynastian aikakaudelta 1600-luvulta. Se oli suunniteltu kauppiaiden käyttöön ja siinä oli seitsemän helmeä seitsemässä pienessä tangossa ja se toimi alkeellisena laskimena kaupankäynneissä nopeita laskutoimituksia varten. (Ometov ym. 2021: 184–185.) Toinen esimerkki on Gulerin, Gannon ja Sicchion (2016) mainitsema 1890-luvulla kehitetty ensimmäisenä kuulolaitteena toiminut korvatorvi. Äänentoiston laadun parantaminen ja korvatorven koon pienentäminen olivat käytettävyyden kannalta oleellisimpia asioita kehittää. Puettavan teknologian historialliseksi edeltäjäksi he esittivät 1500-luvulla kehitetyn rannekellon. Ensimmäinen digitaalinen kello suunniteltiin 1920-luvulla ja 1970-luvulla digitaalinen kello näytti ajan lisäksi päivämäärän sekä siinä oli sekuntikello, ajanotto, hälytys ja valaistu näyttö. 1994 julkaistiin ensimmäinen älykello, joka jo pystyi kommunikoimaan toisen laitteen kanssa. 1950-luvulla debytoi Sonyn ensimmäinen transistoryradio, TR-55. Sony TR-55 toimi mallina nykyisin käyttämillemme kannettaville laitteille, kaiken iPodista Game Boyhyn voi jäljittää TR-55:n muotoiluun.

Samoihin aikoihin Morton Helig loi Telesphere Maskin, ensimmäisen päähän kiinnitettävän näytön, joka tarjosi käyttäjälle 3D-elokuvan ja stereoäänen. Kesti joitakin vuosia, mutta VR-lasit syntyivät lopulta tästä varhaisesta läpimurrosta. (Guler & Gannon & Sicchion 2016: 3–10.)

1960-luvulla astronauttien kypärät sisälsivät tekniikkaa, joka mittasi sykettä ja hengitystä. Vuonna 1961 Edward Thorp ja Claude Shannon loivat oman versionsa puettavasta teknologiasta, tietokoneen joka oli niin pieni, että se mahtui kenkään. Tietokone oli suunniteltu auttamaan heitä huijaamaan rulettipelissä ja se oli ajoituslaite, jolla voitiin ennustaa, milloin ruletin pallo pysähtyy. 1970-luvulla Steve Mann kehitti ensimmäisen puettavan tietokoneen, wearable computer, joka koostui kamerasta, mikrofonista ja kannettavasta tietokoneesta. Hän käytti tätä laitetta tutkiessaan laajennetun todellisuuden käsitettä. Luvun loppupuolella julkaistiin Sonyn Walkman, josta alkoi musiikin ja kannettavan teknologian vallankumous 200 miljoonalla myydyllä laitteella. (Guler & Gannon j& Sicchio 2016: 3–10; Condeco 2018.)

1980-luvulla puettavat älylaitteet saapuivat urheiluun Polar Electron kehittäessä sykemittarin, joka koostui sykevyön lisäksi signaalin vastaanottimesta ranteessa. Vuonna 1987 julkaistiin kuulokojeet, jotka mullistivat terveydenhuoltoalan. 1990-luku toi mukanaan käsi- ja rannetietokeet varastoihin ja logistiikkaan. Nämä sisälsivät lisäksi näytön ja skannerin. Sijainnin seuranta eteni myös tällä vuosikymmenellä, kun Olivetti keksi kannettavan Active Badge-laitteen. Se käytti infrapunasignaaleja henkilön sijainnin määrittämiseen ja sitä voidaan pitää Google Mapsin kaltaisten sovellusten edeltäjänä. 2000-luvun tunnetuin tuote on iPod, se oli askel eteenpäin Walkmanista sillä se vähensi tarvetta hankalille kaseteille tai levyille ja käytti teknologiaa musiikin kuuntelun mahdollistamiseksi missä vain. 2000-luvun alussa yleistyivät myös Bluetooth-kuulokkeet. Niitä käytettiin aluksi puheluiden vastaanottamiseen ja musiikin kuunteluun, lisäksi ne yleistyivät myös urheilun piirissä. (Condeco 2018.)

Fitbitin lanseeraus 2010-luvulla johti älykellojen ja muiden puettavien älylaitteiden räjähdysmäiseen yleistymiseen. Siitä alkoi puettavien älylaitteiden nykyaalto, jossa älypuhelinten kanssa synkronoitavat laitteet sekä IoT tulivat osaksi tavallistenkin ihmisten arkipäivää. (Condeco 2018.)

Puettavan teknologian kehittämisessä on perinteisesti korostettu käytettävyyden merkitystä, jotta laitteet vastaisivat mahdollisimman hyvin käyttäjiensä tarpeisiin ja

olisivat hyväksyttäviä laajemmassa käytössä. Historiallisesti tarkasteltuna laitteiden koon pienentäminen ja niiden tarkkuuden parantaminen ovat olleet keskeisiä näkökohtia niiden kehityksessä ja teknologisessa edistymisessä. (Yli-Länttä 2021: 9.)

2.2 Määritelmä

Puettavilla älylaitteilla tarkoitetaan asusteina käytettäviä tai kehoon kiinnitettäviä, kehoon implantoituja tai tatuoituja, elektronisia laitteita tai vaatteita, joihin on upotettu teknologiaa. Laitteita voidaan käyttää seuraamaan tietoa käyttäjästään sekä suorittamaan monia muita tehtäviä, kuten viestintää, terveyden seurantaa ja liiketoiminnan analysointia. Puettavien älylaitteiden ja puettavan teknologian määritelmä ei ole aivan yksiselitteinen. Rauttola ym. (2019: 3) mukaan puettavaksi teknologiaksi määritellään laitteet, jotka puetaan päälle ja joilla tutkitaan käyttäjän fysiologista tilaa sekä käyttäytymistä yhden tai useamman signaalin avulla. Rajanen ja Weng (2017: 154) määrittelevät, että ylle puettaviin vaatteisiin tai koruihin sijoitetut pienet tietokoneet ovat puettavia älylaitteita. Näissä laitteissa on heidän mukaansa muistin lisäksi kyky kommunikoida käyttäjänsä kanssa. Tämä mahdollistaa tiedon reaaliaikaisen tutkimisen sekä mahdollisuuden lähettää tietoa mobiililaitteelle internetin ylitse, jolloin dataa on mahdollista analysoida tarkemmin. Iqbal, Aydin, Brunckhorst, Dascupta ja Ahmed (2016: 372) määrittelevät puettavan teknologian kompaktiksi käyttäjälleen tietoa esittäväksi laitteeksi, joka mahdollistaa joko fyysisenä syötteenä tai äänikomennuksen avulla vuorovaikutuksen käyttäjän ja laitteen välillä ja ovat yleensä puettavia vaatteita ja asusteita. Tässä opinnäytetyössä puettavalla älyvaatteella tarkoitetaan pienikokoista elektronista laitetta, joka on suunniteltu pidettäväksi kehon päällä, yleensä vaatteiden tai asusteiden osana. Nämä laitteet seuraavat ja tallentavat erilaisia terveys- ja liikuntaan liittyviä tietoja ja ovat integroituna älypuhelimeen tai tietokoneeseen.

Puettavien älylaitteiden jaottelu ei myöskään ole täysin selkeää. Wearable Technologies- kehitysyhtiön perustajan ja toimitusjohtajan Christian Stammelin mukaan puettava älyteknologia voidaan jakaa kuuteen ryhmään. Näitä ovat urheilu-ja fitness-, lääketieteelliset laitteet, lifestyle, muotituotteet sekä teollisuus- ja turvallisuustuotteet. Kun taas Huawein verkotettujen mobiililaitteiden ja kuluttajatuotteiden johtaja Yang Yongin puolestaan jakaa puettavan teknologian sen mukaan, missä kohdassa kehoa sitä käytetään. Näitä ovat silmikot ja virtuaalilasit, rinta- ja käsivarsituotteet, nielaistavat pillerit, kellot, rannekkeet sekä kengät. (Kärkkäinen 2015.)

2.3 Laitteet, käyttötarkoitukset ja toiminnallisuudet

Tänä päivänä melkein mikä tahansa vaate tai asuste voidaan valmistaa puettavana älylaitteena. Laitteista yleisimpiä ja tunnetuimpia ovat älykellot, -lasit, -paidat, -sormukset -housut, ja -kengät. (Vähäkainu & Neittaanmäki 2018: 43–44.) Esimerkkejä näistä on havainnollistettu kuvassa 1. Puettavia älylaitteita hyödynnetään useilla eri tavoilla ja eri aloilla. Puettavien älylaitteiden avulla on usein mahdollista mitata käyttäjän fysiologisia piirteitä (Rajanen & Weng 2017: 154). Tästä syystä niitä käytetään paljon lääketieteessä ja urheilun parissa. Terveydenhuollon teollisuus on tällä hetkellä yksi suurimmista toimijoista, jotka kasvattavat ja kiihdyttävät puettavien älylaitteiden markkinoita. Tämä johtuu sekä kuluttajien että ammattilaisten kiinnostuksesta teknologiaa kohtaan. (Meola 2016.) Lääketieteen ja urheilun lisäksi puettavia älylaitteita käytetään logistiikassa ja teollisuudessa, kuluttajaelektroniikassa sekä sotilas- ja turvallisuusalalla (Cho 2012: 2).

Kuva 1. Yleisimmät puettavat älylaitteet.

2.3.1 Urheilu ja fitness

Kuntoilun seurantasovellukset johtavat markkinoita puettavien älylaitteiden kategoriassa. Useimmat kuluttajat käyttävät puettavaa teknologiaa tallentamaan harjoitteluaan, terveystilastojaan sekä edistymistään. Puettavat älylaitteet keräävät sensorien avulla käyttäjästään dataa, kuten sykettä, askeleita ja kuljettua matkaa. (Meola 2016.) Yksi tunnetuimmista urheilussa käytetyistä puettavista laitteista on älykellot. Älykellot ovat yhdistettyjä laitteita, jotka yleensä toimivat Bluetoothin kautta matkapuhelimeen tai tablet-laitteeseen. Älykelloissa on yleensä näyttö. Kellot näyttävät ajan, urheilusuorituksen, unenlaadun ja monien muiden mittaustulosten lisäksi mm. puhelut, viestit, sääolosuhteet ja kalenterin. Joissakin malleissa on myös mahdollisuus suorittaa maksuja ja käyttää älypuhelinta tai siihen yhdistettyjä smartthings-laitteita etänä. Älyrannekkeissa on usein erilaisia antureita, jotka mittaavat sykkeen, askelmäärän, kuljetun matkan ja unenlaadun. Tiedot tallennetaan älypuhelimeen tai tietokoneeseen, jotta niitä voidaan analysoida ja käyttää terveyden seurantaan. (Ericsson 2017.)

Urheilu- ja kuntoiluälyvaatteet, kuten älykengät, älypaita ja älyhanskat, ovat myös kasvava trendi. Ne voivat olla varustettuina erilaisilla antureilla, kuten syke- tai liiketunnistimilla, tai älylaite tai tietokone voi olla sisällytettynä vaatteeseen. (Vähäkainu & Neittaanmäki 2018: 44). Älyvaatteita käytetään esimerkiksi terveyden seurantaan tai urheilusuorituksen parantamiseen. Urheilulaitteet mittaavat monia erilaisia tietoja, kuten käyttäjän liikkeitä, suoritustasoa ja kalorien kulutusta. Tietoa käytetään parantamaan suoritustasoa, tekemään henkilökohtaisia tavoitteita ja jopa auttamaan urheilijoita välttämään vammoja. Älyhanskat voivat olla varustettuina antureilla, jotka seuraavat käyttäjän liikkeitä ja esimerkiksi kertovat, kuinka hyvin käyttäjä pitää tennismailaa. Älykengissä voi olla antureita, jotka seuraavat käyttäjän kävelyä ja juoksua antaen tietoja käyttäjästään kuten askeleen pituus, askeltiheys ja juoksunopeus. Älyvaatteista saatua dataa käyttäjä voi hyödyntää suunnitellessaan tulevia harjoituksia. (Reeder & David 2016: 273–274.) Älyhousut voivat generoida virtaa muille puettaville älylaitteille, mikä helpottaa niiden käyttöä ilman lataustarpeen muistamista. Älykypärät ovat kypäriä, joissa on älyteknologiaa, ja ovat tarkoitettu esimerkiksi pyöräilyyn, moottoripyöräilyyn tai ratsastukseen. Kypärät voivat sisältää esimerkiksi GPS:n, sisäänrakennetun kommunikaatiojärjestelmän, kameran ja automaattisen hätäkutsun tunnistettuaan kolaroinnin tai putoamisen. (Vähäkainu & Neittaanmäki 2018: 66.)

2.3.2 Lääketiede

Puettavia älylaitteita käytetään sairaaloissa, lääketieteen alan yrityksissä, farmaseuttisissa yrityksissä sekä vakuutusyhtiöissä. Puettavien älylaitteiden lisäksi käytössä on myös iholle kiinnitettäviä, ihon alle laitettavia sekä esimerkkinä implanteista nieltävät pillerit, jotka monitoroivat kehoamme sisältäpäin. Älylaitteita käytetään lääketieteellisissä tarkoituksissa, esimerkiksi verenpaineenmittauksessa sekä EKG:n tallentamisessa. Tämä auttaa potilaita seuraamaan terveyttään ja antaa lääkäreille tärkeää tietoa potilaan tilasta. Puettavista älylaitteista saatavan tiedon avulla sairaalajaksot voivat lyhentyä ja toimivampi avohoito mahdollistua. Ennakoiva terveydenhuolto hyötyy enenevässä määrin päälle puettavasta teknologiasta, sillä käyttämällä laitteita tulevien sairauksien ennakointiin on elintapoihin vielä mahdollista tehdä muutos. (Vähäkainu & Neittaanmäki 2018: 41–42.)

Moni yritys on lanseerannut puettavaa älyteknologiaa edustavan laitteen, tässä muutama esimerkki niistä. Abbott:n Glucose monitoring system, jonka avulla pystyy käyttäjä seuraamaan reaaliajassa veren glukoositasapainoa (Abbott 2017). Kroonisen kivun hoitoon on kehitetty muun muassa Quell Relief-älyvyö, joka lievittää kipua aistihermojen stimuloinnin kautta (Quell 2017). Urbana-Champaignin ja Evanstonin yliopistojen tutkijat Yhdysvaltojen Illinoin osavaltiossa kehittivät ihon pinnalle asennettavan, langattoman veren virtauksen määrittämiseen ja ihon nestetasapainoon perustuvan terveysmonitorin. Laiteessa on 36000 nestemäistä kristallia joustavalla ja pehmeällä alustalla, jotka monitoroivat sydänsairauksia ja ihon terveyttä 24 tuntia päivässä. Muutosten tapahtuessa kristallit vaihtavat väriä ja algoritmien avulla saatu data siirretään terveysraporttiin. (Whiteman 2014.) Lääketieteessä on myös kehitetty laastarin tyylinen biosensori, joka kerää käyttäjästään tietoa suorituskyvystä, sijainnista, liikkumisesta ja kehon toiminnoista EKG-käyrästä lämpötilaan saakka. Mitattu data analysoidaan, kun se on lähetetty langattomiin mobiililaitteisiin ja portaaliin. (Pormerleau 2015.) Embrace Monitor-ranneke monitoroi käyttäjän aktiviteettia lääketieteellisen tarkoilla sensoreilla. Se voidaan esimerkiksi pukea epilepsiaa sairastavan lapsen ranteeseen ja antaa hälytyksen älypuhelimeen, jos lapsi saa kohtauksen. (Kosir 2015.) Puettavat älylaitteet ovat tulossa syöpien havaitsemisen helpottamiseksi. Rintasyöpää skannaavia sensoreita ja älyliivejä on jo markkinoilla. (Vähäkainu & Neittaanmäki 2018: 86.) Leaf-sensori monitoroi ja tallentaa paineen vaihtelua ja potilaan liikkeitä makuuhaavojen ehkäisemiseksi. Se kiinnitetään potilaan

kehoon ja lähettää mitatun datan langattomasti keskusmonitorointijärjestelmään, joka hälyttää hoitajille kun potilas tarvitsee kääntämistä. (Comstock 2015.)

Puettavat älylaitteet voivat myös auttaa käyttäjäänsä unen laadun parantamisessa. Älykellojen ja -rannekkeiden lisäksi unen laadun mittaamiseen on kehitetty älynaamio, joka auttaa ja valmentaa käyttäjäänsä saavuttamaan miellyttävän ja optimaalisen unenlaadun. Tämä Neuro:On älynaamio käyttää valoterapiaa simuloidakseen luonnollisia uniolosuhteita ja mittaa käyttäjänsä sydämen sykettä, silmän liikettä, uniaaltoja ja lihasten jännitystä analysoidakseen ja antaakseen vihjeitä unen laadun parantamiseen. (Vähäkainu & Neittaanmäki 2018: 51.) Älylaitteita on käytetty myös Alzheimerin tautia sairastavien potilainen sijainnin seurantaan (Mahoney & Mahoney 2010: 527–531). Lääketieteellisten puettavien älylaitteiden laajaa käyttöönottoa hidastaa toistaiseksi yksityisyysvaatimukset terveysdatan suhteen sekä laitteiden mittaustulosten epätarkkuus tulosten vertailussa (Meola 2016).

2.3.3 Lifestyle ja muotituotteet

Lifestyle ja muotituotteet jaotteluun kuuluvissa älykoruissa, esimerkiksi sormuksessa tai korvarenkaissa, löytyy samaa teknologiaa ja ominaisuuksia kuin älyrannekkeessa. Älykoruista on kehitetty myös lämpöversioita, jotka voivat lähettää kuumia tai kylmiä pulsseja yleisen lämpötilan kokemisen mukavuuden parantamiseksi käyttäjälleen. (Ericsson 2017.) AR- Tai VR-lasit ovat eräänlainen päähän kiinnitettävä virtuaalitodellisuusnäyttölaite, joka voi sulkea käyttäjänsä näkö- ja kuuloaistit ulkomaailmasta ja saada hänet luomaan kuvitteellisessa ympäristössä olemisen tunteen. Älylaseja voidaan hyödyntää niin lääketieteessä kuin arkielämässäkin. Laseissa on älyteknologian avulla mahdollista tehdä samat asiat kuin älypuhelimella. Älylaseja voidaan esimerkiksi käyttää tekstiviestien ja sähköpostien lähettämiseen, navigoimiseen, kuvien ottamiseen, sekä uutisten että sosiaalisen median ilmoituksien lukemiseen tai esimerkiksi elokuvien katsomiseen. Esimerkiksi Google Glass:a, joka oli ensimmäinen älylasien kaupallinen versio, käytetään äänikomennoilla ja oikeassa sangassa olevalla kosketuspinnalla käsien jäädessä vapaiksi. (Mikkonen 2013.)

2.3.4 Teollisuus- ja turvallisuusala

Teollisuusalalla puettavien älylaitteiden käyttö on kovassa kasvussa. Puettavissa teknologioissa hyödynnetään ratkaisuja kuten ääniohjausta, puheentunnistusta,

erilaisia kameroita ja koodinlukijoita. Laitteisiin voidaan yhdistää erilaisia sovelluksia, joiden avulla tekniikka hyödynnetään työntekijöiden turvaksi, kustannuksia hillitseväksi ja työtä tehostavaksi välineeksi. Laitteiden avulla myös vähennetään tuotantovirheitä sekä parannetaan kunnossapitoa ja ennakoivaa huoltoa. (Neittaanmäki & Lehto & Savonen 2021: 26–30.) Esimerkiksi älylaseja, joihin on integroitu virtuaalinen näyttö ja kamera, käytetään nopeuttamaan ja tarkentamaan tarkastuksia ja korjauksia sekä korvaamaan paperiset versiot esimerkiksi työohjeista. Myös dokumentointi on muuttunut tarkemmaksi ja reaaliaikaisemmaksi laitteiden käytön myötä. Puettavia antureita voidaan käyttää valvomaan työntekijöiden fyysistä kuntoa tai seuraamaan tuotantoprosessien suorituskykyä sekä ennustamaan laitteiden huoltotarpeen ennen kuin laite hajoaa. Näin vähennetään työntekijöiden loukkaantumisriskiä, parannetaan työhyvinvointia, vähennetään käyttökatkoja, helpotetaan laadunvalvontaa, lisätään laitteiden käyttöikää ja optimoidaan tuotantoprosesseja. Esimerkiksi älykypärä voi ratkaista ongelmat tuotantopaikan turvallisen toiminnan prosessissa, toteuttaa havaintoja, palvelua, analysointia, komentoa ja valvontaa. Sen seurantaominaisuutta voidaan käyttää työskenneltäessä vaarallisilla työalueilla, esimerkiksi voimaloissa ja kaivoksissa laitteen kertoessa turvarajat. (Yadav & Mishra & Das 2015: 330–333.) Puettavia älylaitteita voidaan käyttää myös vaikkapa fyysisesti raskaissa nostoja vaativissa työtehtävissä apuna. Puettavat älylaitteet ovat tärkeitä myös sotilas- ja turvallisuusaloilla, joissa niitä käytetään tiedusteluun, hälytyksen tekemiseen, pelastustoimintaan ja vaarallisten tehtävien suorittamiseen. (Pomerlau 2015.)

Liiallinen istuminen ja fyysisen passiivisuus ovat terveysriskejä, johon puettavat älylaitteet voivat puuttua muistuttamalla työntekijää liikkumaan. Työpaikoilla puettavia älylaitteita voidaan käyttää muun muassa monitorointiin, avustuksen, sisällön toimittamiseen ja seurantaan. Työnantaja pystyy panostamaan työntekijöiden hyvinvointiin saamalla laitteiden avulla tietoa heidän fyysisestä kuormittumisestaan sekä mielialastaan. (Khakurel & Melkas & Porras 2018: 791–818.)

2.4 Tiedonvälityksessä käytetyt teknologiat

Puettaville älylaitteille on tyypillistä tiedon verkkoon välitys jonkin yhdyskäytävänä (Gateway) toimivan laitteen, useimmiten älypuhelimen, välityksellä. Älylaitteiden tiedonvälityksessä käytetään tällä hetkellä useita teknologioita, yksinään tai yhdistettynä, jotka mahdollistavat laitteiden välisen kommunikoinnin ja datan siirron. Näitä ovat muun muassa Bluetooth Low Energy eli BLE, ANT/ANT+, ZigBee ja NFC.

Vanhimmat älylaitteet, kuten Fitbit, käyttivät Ant/Ant+-protokollaa tiedonsiirtoon rannekkeen ja telakan välillä. ZigBee on erityisesti lääketieteellisiin tarkoituksiin suunnitelluissa puettavissa älylaitteissa ja BLE on vähäisen virrankulutuksen vuoksi muodostunut yleisimmin käytetyksi älylaitteen ja älypuhelimen tai älylaitteen ja langattomien kuulokkeiden ja muiden pienten laitteiden välillä käytetty oleva lyhyen kantaman radioteknologia. NFC (Near Field Communication) on teknologia, joka mahdollistaa laitteiden välisen tiedonsiirron lyhyellä etäisyydellä toisistaan ja NFC-tekniikkaa käytetään usein maksamiseen ja kulkulupien käyttöön. Älylaitteen käyttäjä on yleensä asentanut älypuhelimeensa sovelluksen, johon data laitteesta siirtyy. Tämä sovellus välittää kerätyn datan verkkopalvelimelle analysoitavaksi, josta se lähetetään takaisin käyttäjän sovellukseen esitettäväksi. Langaton verkko (Wi-Fi) on tällä hetkellä eniten käytetty teknologia, joka mahdollistaa nopean langattoman yhteyden ja kommunikoinnin älylaitteiden ja Internetin välillä. Älykellot ja rannekkeet mahdollistavat myös toisen suunnan kommunikaation muun muassa välittämällä puhelut, teksti- ja sähköpostitviestit käyttäjän älypuhelimesta. (Seneviratne ym. 2017.)

Viides sukupolvi langattomia verkkoja (5G) mahdollistaa erittäin nopean tiedonsiirron ja alhaisen viiveen, mikä on tärkeää monille älylaitteille, kuten esimerkiksi autonomisille ajoneuvoille ja muille IoT-laitteille. Satelliittiyhteyksiäkin käytetään, mutta vain kun muita yhteyksiä ei ole saatavilla tai kun yhteyden on oltava käytettävissä laajalla alueella. Satelliittiyhteydet ovat tärkeitä erityisesti maaseudulla tai muilla syrjäisillä alueilla sekä puolustusvoimien käytössä. (Ometov ym. 2021: 184–185.)

Vaikka puettava älyteknologia tarjoaa merkittäviä hyötyjä, sen käyttöön liittyy myös riskejä. Kun teknologia kehittyy, tietojen mahdollinen vuotaminen ja luvaton käyttö muodostuvat kasvaviksi huolenaiheiksi. Älylaitteet, jotka ovat jatkuvasti yhteydessä verkkoon, ovat erityisen alttiita kyberuhkille, kuten haittaohjelmille, tietomurroille ja luvattomille pääsyille. Laitteet ovat yhä kehitysvaiheessa ja niiden luotettavuuteen kohdistetaan optimistisia odotuksia. Käyttäjät ovat tällä hetkellä halukkaita jakamaan tietoa kolmannen osapuolen palveluntarjoajille, jos kokevat saavansa siitä jonkinlaista hyötyä. Käyttäjistä yli 60 % tuntee voivansa kontrolloida sitä, kenelle tietoa jaetaan sekä tuntevat tietojensa olevan turvassa. Eniten käyttäjät ovat valmiita jakamaan tietojaan laitevalmistajille, terveys- ja kuntoilupalvelujen tarjoajille, vakuutusyhtiöille ja terveydenhuollon ammattilaisille, vähiten työnantajille. (Ericsson 2017.)

2.5 Esineiden internet

Internet of Things (IoT) -käsitteen käännös suomeksi on esineiden tai asioiden Internet. Tämä tarkoittaa järjestelmää, jossa toisiinsa liittyneet tietotekniset laitteet voivat kerätä ja siirtää tietoa automaattisesti langattoman verkon kautta. Esineiden Internetille ei ole olemassa yksittäistä yleisesti käytössä olevaa määritelmää, vaan termiä käytetään laaja-alaisesti teknologiasta puhuttaessa sekä kehitettyjen palveluprototyyppien markkinoinnissa. (Ryynänen 2016.)

IoT on kokonaisuus, jossa jokainen laite tai sensori on yksilöitävissä (sillä on IP eli Internet Protocol-osoite), se on yhteydessä internetiin, reagoi ympäristön muutoksiin sekä kykenee välittämään tietoa toiselle laitteelle. Internetin avulla esineet koko ajan välittävät, tallentavat ja analysoivat keräämäänsä dataa reaaliajassa. Täydellinen IoT-järjestelmä koostuisi neljästä erillisestä elementistä eli sensoreista tai laitteista, yhteyksistä, tietojenkäsittelystä sekä käyttöliittymästä. IoT:tä ei ole vain kannettavat tietokoneet tai älypuhelimet vaan päälle/poiskytkimellä varustettu, melkein mikä vaan sensori tai laite, jossa datan käsittelyn, laskentatehon, verkkoyhteyden ja ohjelmiston osalta vaatimukset täyttyvät. Esineet on varustettu erilaisilla sensoreilla, toimilaitteilla ja tunnisteilla, joiden avulla ne havainnoivat ja keräävät dataa ympäristöstään. Jatkuva kehitys piiri- ja viestintäteknologiassa mahdollistaa internettiin liitettävien laitteiden variaation pienistä mittausanturi- ja kodin kulutuselektroniikkalaitteista aina teollisuuden vaativassa käytössä oleviin työkoneisiin saakka. Esimerkkejä IoT mahdollisuuksista ovat mm. nykyaikaiset älykellot, joilla voit maksaa kaupassa, kuljetusautojen etäohjaus sekä niiden lämpötilan ja kosteuden etävalvonta, sähkömittareiden etäluenta, kannettava EKG-laitteisto, ilmastoinnin etäsäätö rakennuksissa, käyttäjäänsä lääkkeenotosta muistuttava ja lääkkeiden ottamista valvova lääkepurkki tai huollon tarpeesta ilmoittava kodinkone. (Atzori ym. 2020: 2791.)

IoT on ihmisten ja esineiden tai sovellusten välisen kommunikoinnin uusien ratkaisujen kautta tapahtuva laajennus, joka mahdollistaa yhteyden joko ihmisen ja esineen välillä, esineen ja esineen välillä tai useiden esineiden välillä. Olennaista on myös infrastruktuuri, jonka avulla esineiden Internetiin liittyvä tieto kerätään, tallennetaan ja jaetaan. Tiedon välittämiseen esineet käyttävät muun muassa radiotaajuista etätunnistamista, langattomia sensoriverkkoja ja mobiiliverkkoa. (Atzori ym. 2020: 2791.) Jatkuva internetyhteys ja pilvipalvelut ovat pääroolissa kerätyn datan tallennuksessa paikkaan, josta se on jaettavissa muille laitteille. Piirien laskentatehon

kasvu ja samanaikainen fyysisen koon pieneneminen ovat mahdollistanut uusien laskenta-algoritmien käytön datan käsittelyyn erittäin pienissä laitteissa. Kasvava tiedonsiirtokapasiteetti mahdollistaa suurten tietomäärien keräämisen ja jalostamisen käyttökelpoiseen muotoon, mikä tuo enemmän hyötyä tuotanto- ja liiketoiminnalle. Langaton viestintä on yksi keskeisimmistä tekijöistä IoT:n tulevaisuuden kasvussa ja yleistymisessä. (Verronen & Kaartinen & Nokela 2016: 12–13.)

Puettavia älylaitteita on kutsuttu yhdeksi isoimmista IoT-sovelluksista. IoT:n kehitys alkoi 1990-luvun lopulla, mutta vasta viime vuosikymmenen aikana sen merkitys on lisääntynyt huomattavasti. Esineiden internet on tällä hetkellä voimakkaasti kasvussa johtuen langattomien verkkoteknologioiden kehittymisestä sekä halvemmista antureista ja sensoreista, mikä avaa laajoja liiketoimintamahdollisuuksia. Tällä hetkellä IoT:n ratkaisuille haasteita ja jopa ongelmia aiheuttaa langattomien verkkojen tietoturva ja laitteistojen toimintaan tarvittava virran määrä. (Meola 2016.)

3 Puettavien älylaitteiden tietoturva

3.1 Historia

Tietoturvan alkuvaiheet ulottuvat antiikin aikoihin, jolloin salakirjoitus oli ensimmäinen keino suojata tärkeitä viestejä ulkopuolisilta. Yksi tunnetuimmista menetelmistä on Caesarin salakirjoitus, joka perustui kirjainten korvaamiseen toisilla kirjaimilla aakkosjärjestyksessä. Toisen maailmansodan aikainen salakirjoitustekniikka, erityisesti saksalaisten Enigma-kone, oli merkittävä edistysaskel tietoturvan historiassa. Enigman purkaminen ei ainoastaan auttanut liittoutuneita voittamaan sotaa, vaan se myös asetti perustan modernille kryptografialle. 1940- ja 1950-luvuilla, tietokoneiden alkuaikoina, koneet olivat suuria ja monimutkaisia, ja tietoturva keskittyi pääasiassa fyysiseen suojaamiseen. Tietokoneiden ja internetin leviäminen laajemmalle 1970-luvulla loi tarpeen kehittyneemmille tietoturvaratkaisuille. UNIX-käyttöjärjestelmän kehittäminen toi mukanaan käyttäjien todennuksen ja tiedostojen pääsyn valvonnan. (Miettinen 2002: 4–6.)

Tietokonevirukset, kuten 1970-luvun Creeper ja Reaper, osoittivat kyberuhkien todellisuuden. 1990-luvulla tietoturvan merkitys kasvoi entisestään, kun digitaalinen infrastruktuuri laajeni ja sähköisen kaupankäynnin kasvu ja henkilökohtaisten tietojen

suojaamisen tarve johtivat uusien tietoturvan standardien ja protokollien, kuten SSL:n (Secure Sockets Layer), kehittämiseen. 2000-luvun myötä kyberrikollisuus nousi merkittäväksi globaaliksi uhaksi. Identiteettivarkaudet, tietojenkalastelu-hyökkäykset ja tietomurrot olivat esimerkkejä uudenlaisista haasteista, joita tietoturva-asiantuntijat kohtasivat. Tämä aika merkitsi tietoturvan kehittymistä pelkästä suojauksesta monimutkaiseen kokonaisuuteen, joka sisältää uhkien torjunnan, tietosuojan, tietojen eheyden ylläpidon ja käyttäjien valtuutusten hallinnan. (Miettinen 2002: 12.)

3.2 Nykytila ja määrittelyä

Nykyään tietoturva on keskeinen osa kaikkia digitaalisia prosesseja. Kehittyneet tekniikat, kuten tekoäly ja koneoppiminen, ovat tulleet tärkeiksi työkaluiksi uhkien havaitsemisessa ja torjunnassa. Tietoturvan historia heijastaa teknologian kehityksen ja yhteiskunnallisten tarpeiden välistä vuorovaikutusta, ja sen merkitys kasvaa koko ajan digitaalisen maailman jatkuvasti kehittyessä. Kyberturvallisuus on jatkuvasti kehittyvä kenttä, jossa uudet teknologiat ja uhkamallit vaativat jatkuvaa sopeutumista ja innovaatiota. (Miettinen 2002: 9.)

Tietoturva on termi, jolla tarkoitetaan tiedon, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Se viittaa toimenpiteisiin, käytäntöihin, tekniikoihin ja prosesseihin, joilla suojataan muun muassa tietoja, tietojärjestelmiä, tietoliikennettä ja tietoverkkoja luvattomalta pääsyltä, käytöltä, vahingoittamiselta tai paljastamiselta. Tietoturva tarkoittaa esimerkiksi teknisiä ja organisatorisia toimenpiteitä, joilla taataan järjestelmien käytettävyys, datan eheys ja luottamuksellisuus sekä rekisteröidyn oikeudet ja niiden toteutuminen. Tietoturvalla ja tietoturvallisuudella tarkoitetaan myös tilaa, jossa tietoturvariskit ovat hallinnassa. Puettavat älylaitteet keräävät, tallentavat ja lähettävät henkilökohtaisia tietoja käyttäjistään. Tämä herättää huolen tietoturvasta ja yksityisyydensuojasta. Tietoturva on yksi tietosuojan toteuttamisen keino. (Seneviratne ym. 2017; Muurinen 2019.)

Perinteisesti on ajateltu tietoturvan koostuvan kolmesta tavoitteesta, eli tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Tiedon luottamuksellisuudesta (confidentiality) huolta pitämisellä tarkoitetaan sitä, että tietoa eivät ulkopuoliset pääse katselemaan ja sitä käsittelevät vain siihen oikeutetut henkilöt. Eheydestä (integrity) huolta pitämisellä tarkoitetaan sitä, että tiedot eivät muutu tahattomasti ilman valtuutettujen henkilöiden toimia tai hyökkäyksen seurauksena ja että kaikki muutokset

ovat havaittavissa. Eheys voidaan myös määritellä niin sanotuksi sisäiseksi eheydeksi, eli tietojen loogisuudeksi ja ulkoiseksi eheydeksi eli paikkansapitävyydeksi. Tietojen saatavuudesta (availability) huolta pitäminen tarkoittaa, että tieto on tarpeen tullen saatavilla. Nykyään näitä kolmea ajatellaan täydentävän kiistämättömyys (non-repudiation), eli tekemäänsä tekoa ei voi henkilö kiistää, tunnistus (identification) jossa tietojärjestelmän käyttäjä pystytään liittämään käyttäjätunnukseensa sekä todennus (authentication), jonka avulla tietojärjestelmän käyttäjä pystytään tunnistamaan oikeus- tai luonnolliseksihenkilöksi. (Seneviratne ym. 2017; Muurinen 2019.)

3.3 Käyttäjätiedon keräämisen laajuus

Niin puettavat älylaitteet kuin IoT-laitteetkin keräävät käyttäjästään paljon tietoa, jolloin riski laitteen käyttäjän henkilökohtaisiin yksityistietoihin pääsyyn kasvaa (Weber 2015: 619). On tärkeää suojella erityisesti seuraavia tietoja: henkilökohtaiset tiedot kuten nimi, osoite ja muut henkilöllisyyttä määrittelevät tiedot, sijaintitiedot, jotka paljastavat käyttäjän liikkeet reaaliajassa tai historiallisesti, sekä terveydentilatiedot, kuten sydämen syke ja verenpaine. Myös viestintätiedot, kuten puhelut ja tekstiviestit, kuluttajatottumukset, kuten ostoshistoria, sekä biometriset tiedot, kuten sormenjäljet ja kasvojen tunnistetiedot, ovat herkkiä ja vaativat suojelua. Laitteiden keräämiä tietoja esitetty kuvassa 2, tietoja, joita käyttäjästä kerätään. Lisäksi laitteiden välisen verkkoliikenteen tiedot ja sovellusten käyttötiedot, kuten sovellusten käyttöajat ja asetukset, ovat arkaluontoisia ja niiden suojaamiseen tulee kiinnittää erityistä huomiota. (Härkönen & Suomalainen & Vänskä 2020.)

Kuva 2. Tietoja, joita käyttäjästä kerätään (Soveltaen: Härkönen & Suomalainen & Vänskä 2020; Mediakasvatusseura 2019).

IoT-laitteet ovat yhteydessä toisiinsa suurimmaksi osaksi näkymättömällä vuorovaikutuksella, jolloin riskien tunnistaminen on entistä hankalampaa. IoT-laitteet keräävät tietoja puettavien älylaitteiden lisäksi monesta eri kohteesta yhdistäen nämä massadatan avulla muodostaen henkilöstä profiilin tyyppisen tiedoston. (Weber 2015: 619.) Yksityishenkilön käyttäytyminen voidaan identifioida näiden tietojen avulla (Watts 2016: 58). Suojelun tarve korostuu, sillä kerätty data, käyttäjästä koostettu informaatio, sisältää muun muassa kulutustottumuksista, terveydestä ja sijainnista tietoa. Tietoa käytetään monin tavoin, kuten käyttäytymiseen perustuvassa mainonnassa, ja sitä voidaan myydä eteenpäin datakauppiaille. (Härkönen & Suomalainen & Vänskä 2020; Watts 2016: 58.) Puettavien älylaitteiden tietoturvaa hankaloittaa tekniikan nopea edistyminen ja alan kasvu, tietoturvan sääntely laahaa koko ajan kehityksen jäljessä. IoT-laitteen käyttäjä ja tarjoaja saattavat molemmat olla tietämättömiä siitä, että laitteesta puuttuu tietoturvasuojaus. Tämä muodostuu yksityisyydensuojan takaamisen ongelmaksi, jos ei laitteiston päivitykset enää ole ajan tasalla. (Folk & Hurley & Kaplow & Payne 2015: 4.)

3.4 Vaatimukset ja lainsäädäntä

Puettavien älylaitteiden suosion kasvaessa niiden tietoturvaan liittyvät riskit ovat nousseet tärkeään asemaan. Tietoturva on moniulotteinen kysymys, joka liittyy tiiviisti sekä käyttäjien henkilökohtaisiin että terveystietoihin. Tällä alueella sovellettava lainsäädäntö, määräykset ja säädökset muodostavat monimutkaisen kokonaisuuden, jonka tarkoituksena on varmistaa tietojen suojaus sekä mahdollistaa innovatiivisen teknologian kehittäminen. Nämä lainsäädännölliset ja standardeihin liittyvät vaatimukset koskevat laitteiden turvallisuutta, yksityisyyden suojaa ja käytettävyyttä. (Valtioneuvoston Luoti-julkaisu 2006.)

Suomessa puettavien älylaitteiden markkinoita ja datan keräämistä säätelevä lainsäädäntö pohjautuu tällä hetkellä toisistaan irrallisiin säädöksiin, kuten Euroopan unionin yleiseen tietosuoja-asetukseen (General Data Protection Regulation, GDPR) ja sopimusoikeuteen (varallisuusoikeudellisia oikeustoimia koskeva laki 13.6.1929/228), joten kokonaiskuva ja normien soveltuvuus on epäselvää. Lainsäädännön hajanaisuus on antanut yrityksille mahdollisuuden luoda itse omat sääntönsä ja datan hallinta perustuu tällä hetkellä niiden itse laatimiin vakioehtoisiin sopimuksiin. Puettavien älylaitteiden käyttäjät yleensä joutuvat hyväksymään käyttöoikeussopimuksen ennen laitteen käyttöönottoa. GDPR asettaa viitekehyksen henkilötietojen käsittelylle, korostaen henkilötietojen suojauksen tärkeyttä. GDPR:n vaatimukset ovat erityisen tärkeitä puettavien älylaitteiden kohdalla, koska ne keräävät käyttäjistä henkilökohtaista dataa, joka voi olla hyvin arkaluonteista. GDPR velvoittaa yrityksiä noudattamaan tiukkoja tietojenkäsittelyn standardeja ja vaatii selkeää suostumusta tietojen keräämiseen ja käyttöön. Yhdysvalloissa vastaavaa tietosuojaa ohjaa terveydenhuollon tietosuojaa ja vastuuta koskeva laki (The Health Insurance Portability and Accountability Act, HIPAA), joka säätelee terveystietojen käsittelyä. Lisäksi kuluttajansuojaa valvovat eri maissa erilaiset elimet, kuten Yhdysvaltain Federal Trade Commission (FTC), joka asettaa standardeja markkinoinnille ja yksityisyyden suojalle. Myös tietoliikenne- ja radiolaitteiden standardeja ja vaatimuksia on määritelty eri maissa ja alueilla. (Harenko & Niiranen & Tarkela 2016: 71.)

Teknisten standardien osalta Bluetooth Special Interest Group (Bluetooth SIG) tarjoaa määrittelyjä Bluetooth-teknologialle, joka on keskeinen elementti puettavien laitteiden langattomassa kommunikaatiossa. ISO/IEC-standardit, erityisesti ISO/IEC 27000-sarja, tarjoavat laajan kehyksen tietoturvan hallinnalle, jota sovelletaan myös älylaitteissa.

(Bluetooth 2015: 1.) Euroopan talousalueella myytävien laitteiden on oltava myös CE-merkittyjä, mikä osoittaa laitteiden täyttävän EU:n asettamat turvallisuus- ja ympäristöstandardit (Grönlund ym. 2017).

Edellä mainittujen lisäksi EU:ssa on kehitetty säädöksiä, kuten Digimarkkinasäädös (Digital Markets Act eli DMA) ja Digipalvelusäädös (Digital Services Act eli DSA), jotka tukevat digitaalisten markkinoiden ja palveluiden turvallista kehitystä ja käyttöä. Datanhallinta-asetus (Data Governance Act eli DGA), Tekoälysäädös (Artificial Intelligence Act eli AIA) ja Datasäädös (Data Act) ovat esimerkkejä EU-tasoisista toimenpiteistä, jotka edistävät tietojen turvallista käsittelyä ja käyttäjien yksityisyydensuojaa. eIDAS-asetus (Electronic identification, authentication and trust services) puolestaan tarjoaa kehyksen sähköisille identiteeteille, mikä on olennaista puettavien älylaitteiden käyttäjille. Avoimen datan direktiivi (EU 2019/1024) edistää julkisten tietojen avoimuutta ja uudelleenkäyttöä mahdollistaen innovaatiot puettavien laitteiden alalla. Säädökset luovat yhdessä kehyksen, joka ohjaa puettavien älylaitteiden kehitystä, markkinointia ja käyttöä, määritellen kuinka dataa kerätään, käsitellään ja jaetaan sekä miten kuluttajien oikeuksia suojataan digitaalisessa ympäristössä. (Euroopan komissio 2024; Laaksonen 2020: 2–4.)

Puettavat älylaitteet keräävät käyttäjän terveyteen liittyvää tietoa, mutta ne tulee erottaa lääkinnällisistä laitteista, joita säädellään erillisellä lainsäädännöllä (esim. Laki terveydenhuollon laitteista ja tarvikkeista, 24.6.2010/629) ja joiden markkinointia ja turvallisuutta valvovat viranomaiset kuten Fimea ja Valvira. Lääkinnällisinä laitteina säänneltyihin ratkaisuihin sovelletaan useita velvoitteita, joilla taataan laitteiden ja sovellusten toimivuus aiottua käyttötarkoitusta varten ja siten myös laitteen tai sovelluksen antamien tietojen laadun. Lääkinnällisiä puettavia laitteita sääntelevät tarkat määräykset, sillä niiden osalta on noudatettava Medical Device Regulation (MDR) -asetusta EU:ssa. Se määrittelee, millaiset lääkinnälliset laitteet saavat olla markkinoilla ja miten niitä tulee testata ja hyväksyä. Kuluttajien fyysisen turvallisuuden varmistamiseksi Yhdysvaltain Consumer Product Safety Commission (CPSC) on luonut turvallisuusstandardeja, jotka ohjeistavat puettavien laitteiden suunnittelua ja tuotantoa. Monet hyvinvointituotteet jäävät kuitenkin lääkinnällisiä laitteita koskevien asetusten soveltamisalan ulkopuolelle, sillä niiden käyttötarkoitus ei ole lääketieteellinen. EU on vastannut tähän ongelmaan ”soft law” tyyppisin keinoin, joista viimeisimpänä on vuonna 2021 julkistettu ISO/TS 82304- 2 standardi

terveysohjelmistojen laatustandardeista. (Euroopan komissio 2024; Laaksonen 2020: 5–8.)

EU:n vaatimukset puettavien älylaitteiden tietosuojan osalta ovat tiukentumassa, erityisesti uuden radiolaitedirektiivin myötä. Tämä direktiivi koskee kaikkia internetiin suoraan tai toisen laitteen kautta liitettäviä langattomia laitteita, kuten älykelloja, matkapuhelimia, leluja ja WLAN-laitteita. Radiolaitedirektiivi asettaa yhtenäiset vaatimukset radiotaajuuksilla toimiville langattomille laitteille Euroopan markkinoilla. Sen keskeisenä tavoitteena on varmistaa, että nämä langattomat laitteet täyttävät tiukat tekniset vaatimukset eivätkä häiritse muita laitteita radiotaajuuksien käytössä. Direktiivin myötä laitevalmistajien on investoitava huomattavasti enemmän laitteidensa tietoturvaan ja noudatettava tiukempia vaatimuksia. Radiolaitedirektiivin mukaan kaikkien markkinoille saatettavien langattomien laitteiden on täytettävä EU:n yhtenäiset tietoturvavaatimukset viimeistään 1. elokuuta 2024 mennessä. Direktiivin sisältö ei ole olennaisesti muuttumassa, mutta siihen liittyviä harmonisoituja standardeja tarkennetaan parantamaan kuluttajien yksityisyyden suojaa ja varmistamaan viestintäverkkoa ja sen toimintavarmuutta. Radiolaitedirektiivi koskee kaikkia internetiin liitettäviä langattomia laitteita ja luo yhtenäiset vaatimukset niiden tietoturvallisuudelle. Tämä muutos merkitsee suurta haastetta laitevalmistajille, mutta samalla se edistää tietoturvan yhdenmukaistamista Euroopassa ja parantaa kuluttajien suojaa sekä verkkojen vakautta. Radiolaitedirektiivi on osa laajempaa pyrkimystä luoda turvallisempi ja yhdenmukaisempi ympäristö langattomien laitteiden käytölle EU:ssa. (Juutinen haastattelu 14.2.2022 & Keinonen 2022.)

Kansainvälisesti tietoturvan merkitys on tunnustettu ja Suomi on toiminut edelläkävijänä älylaitteiden tietoturvan sertifiointiprosessissa. Suomessa on otettu käyttöön vapaaehtoinen Tietoturvamerkki, jonka Liikenne- ja viestintävirasto Traficom myöntää. Merkki auttaa kuluttajia tunnistamaan tietoturvallisemmat älylaitteet ja edistää yleistä tietoisuutta tietoturvasta. Tietoturvamerkin saaneet tuotteet on testattu ja ne täyttävät tietyt tietoturvaan liittyvät vaatimukset. Merkin tavoitteena on lisätä kuluttajien luottamusta ja auttaa heitä tekemään turvallisempia ostopäätöksiä. (Traficom 2023.)

4 Opinnäytetyön tarkoitus, tavoitteet ja tutkimuskysymys

Puettavat älylaitteet ovat jatkuvasti yhteydessä internetiin, ne keräävät, tallentavat ja siirtävät henkilökohtaista tietoa altistuen erilaisille tietoturvariskeille. Opinnäytetyön tarkoituksena on selvittää, mitä tietoturvariskejä puettavat älylaitteet sisältävät ja tunnistaa tekijät, jotka vaikuttavat näiden laitteiden tietoturvariskeihin. Opinnäytetyö pyrkii tuottamaan kattavan ja ajantasaisen katsauksen aiheesta.

Tavoitteena on lisätä käyttäjien, valmistajien ja muiden sidosryhmien tietoisuutta puettavien älylaitteiden tietoturvariskeistä ja niiden merkityksestä käyttäjälle. Opinnäytetyön tuloksia voivat hyödyntää kaikki terveydenhuollon toimijat, laitteiden valmistajat ja tutkijat, jotka osallistuvat digitaalisen terveydenhuollon kehittämiseen ja käyttöön.

Tutkimuskysymys:

Mitkä ovat yleisimmät puettaviin älylaitteisiin liittyvät tietoturvariskit?

5 Kirjallisuuskatsaus opinnäytetyön menetelmänä

5.1 Menetelmälliset lähtökohdat

Kirjallisuuskatsaus on systemaattinen tutkimusmenetelmä, jonka perustana on prosessimainen tieteellinen toiminta. Kirjallisuuskatsauksessa aiheesta löydetyistä tutkimuksista yhteen kokoamalla muodostetaan tiettyyn asiakokonaisuuteen tai aihealueeseen liittyen kokonaiskuva. Kirjallisuuskatsauksen on oltava toistettavissa ja sen tekijältä edellytetään aihealueensa tuntemusta. Katsauksen tavoitteena on systemaattisuus ja sen vaiheet on oltava kuvattuna tavalla, jolla lukijan on mahdollista arvioida toteutustapaa sekä luotettavuutta jokaisessa eri vaiheessa. (Stolt & Axelin & Suhonen 2016: 7.)

Menetelmä aineiston hankintaan tässä opinnäytetyössä on kuvailevan kirjallisuuskatsauksen alatyyppi, scoping katsaus. Scoping katsauksessa pyritään saamaan kuva tutkittavasta aiheesta olemassa olevan tutkimustiedon avulla. Scoping

katsauksen etuna on, että sen avulla voidaan saada tietoa laaja-alaisesti tutkittavasta aiheesta ja arvioida onko tutkittua tietoa riittävästi. Scoping katsaus tarkastelee aiheesta tehtyjä artikkeleita menetelmästä riippumatta. Se sopii erilliseksi menetelmäksi erityisesti, jos tutkittava aihe on monimuotoinen tai monitahoinen. Tavallisesti scoping katsaus ei sisällä aineiston laadun arviointia. (Stolt & Axelin & Suhonen 2016: 10–11.)

Tämä tutkimusaihe, puettavien älylaitteiden tietoturvariskit, on äärimmäisen ajankohtainen ja monitahoinen. Se vaatii lähestymistapaa, joka mahdollistaa aiemman tiedon kokoamisen ja arvioinnin eri näkökulmista. Scoping katsaus mahdollistaa tämän laajan aineiston kokoamisen ja analysoinnin kattavasti, jotta voidaan muodostaa kokonaiskäsitys puettavien älylaitteiden tietoturvariskeistä. Menetelmänä scoping katsaus sopii käytettäväksi ajankohtaiseen aiheeseen, josta on julkaistu lähiaikoina paljon artikkeleita ja tutkimustietoa. (Suhonen & Axelin & Stolt 2016: 10–11.) Scoping-katsaus on ihanteellinen lähestymistapa puettavien älylaitteiden tietoturvariskien kartoittamiselle, sillä menetelmä on joustava ja kykenee integroimaan sekä uusimman tutkimuksen että monipuolisen aineiston, kuten tässä opinnäytetyössä harmaan kirjallisuuden, antaen mahdollisuuden aiheen kattavaan tarkasteluun. Puettavien älylaitteiden tietoturvan tutkimusalalla standardit ja käytänteet kehittyvät jatkuvasti ja aiheen ajankohtaisuuden vuoksi siitä on julkaistu lähiaikoina paljon artikkeleita ja tutkimustietoa.

5.2 Tiedonhakuprosessin kuvaus, tietokannat ja hakulausekkeet

Scoping katsauksen tiedonhakuprosessi aloitettiin tekemällä alustavaa tiedonhakua eri tietokantoihin, muun muassa MetCat Finnaan ja Google Scholariin, oikeiden hakusanojen tunnistamiseksi, hakulausekkeiden muodostamiseksi ja tietokantojen valitsemiseksi. Haku aloitettiin MeTCat Finnasta jonka perusteella lopulliset haut suoritettiin Cinahl-, ProQuest Central- ja PubMed-tietokannoista. Vaikka aineistoksi valittiin julkaistut ja vertaisarvioidut artikkelit ja vertaisarviointi oli myös haun rajauksena, silti aineiston valinnan ja läpikäynnin välisenä aikana tietokannoista poistui yhteensä kuusi jo aiemmin katsausta varten valittua artikkelia. Osalla näistä poistoista syyksi ilmoitettiin vertaisarvioinnissa ilmenneet epäselvyydet, kun taas osan syytä ei ilmoitettu. Tästä syystä mukaan otettiin myöhemmin myös IEEEXplore-tietokanta aineistomäärän ja laadun kasvattamiseksi. Asiasanastoa tähän kirjallisuuskatsaukseen haettiin koehauilla sekä MESH-sanaston avulla hakulausekkeiden muodostamiseksi.

Lopulliset hakusanat määriteltiin PICO-mallin (patient/population/problem, intervention, comparison, outcome) avulla (taulukko 1.)

Taulukko 1. Asiananastoa PICO-mallin mukaan

Population/**Problem**	Intervention	Comparison	Outcome
Tietoturvallisuus Tietoturva-asetukset Tietoturvaratkaisut Salausmenetelmät Tunnistusmenetelmät Varmistusmekanismit Tietoturvan hallinta menetelmät Riskien hallinta Tietoturvakäytännöt Tietoturvapolitiikka Tietoturvamääräykset Henkilötietojen suojaus Uhkien torjunta	Puettava älylaite Puettava teknologia Puettavat teknologialaitteet Älykellot Älyrannekkeet Älyvaatteet Puettava elektroninen laite Puettava laite Päällepantavat elektroniset laitteet Päällepantavat laitteet Päällepantavat älylaitteet		Tietoturvariski Tietovuodot Haittaohjelmat Tietojenkalastelu Tietoturva-aukko Identiteettivarkaudet Tietojen muuttaminen Tietojen kadottaminen Haavoittuvuudet Turvatoimet
Security settings Security solutions Encryption methods Identification methods Verification mechanisms	Wearable Wearables Wearable devices Wearable smart devices Wearable technology devices Smartwatches Smartbracelets Smart clothing Smart glasses Smart shoes Smart devices Wearable electronic devices Smart textile Smart clothing Smart wearable Smart ppe Electrotextile E-textile Telemedicine Wearable sensor Digital health device Wearable technology		Security risks Data breaches Malware Phishing Identity theft Data manipulation Data loss Computer security Cyber security Cybersecurity Security Cyber safety Privacy

Olennainen osa hakustrategiaa on sisäänotto- ja poissulkukriteerien määrittäminen. Kriteerit ohjaavat tutkimusten valinnassa tarkasteltaessa ensin otsikkotasolla, sitten abstraktitasolla ja lopuksi kokotekstejä. (Niela-Vilén & Hamari 2016: 26–27.) Sisäänotto- ja poissulkuktiteerit määritettiin ennen aineiston hakua, kriteerit on kuvattu taulukossa 2.

Taulukko 2. Aineiston haussa käytetyt aineiston sisäänotto- ja poissulkukriteerit

Sisäänottokriteeri	**Poissulkukriteeri**
-Tutkimusartikkelin tulee olla suomen tai englanninkielinen -Koko tutkimusartikkelin tulee olla saatavilla -Artikkeli on vertaisarvioitu -Tieteellinen tutkimusartikkeli, muu tieteellinen tutkimus tai julkaisu, pro gradu, väitöskirja -Tutkimukset, joiden otsikossa mainitaan sanat ”wearable” ja ”security tai privacy” ja jotka vastaavat tutkimuskysymykseen	-Muu kuin suomen ja englannin kieli -Aineistoa ei ole kokonaan saatavilla -Artikkelia ei ole vertaisarvioitu -Aineisto ei ole tieteellinen tutkimusartikkeli -Aineisto ei vastaa tutkimuskysymykseen eikä otsikossa mainita sanoja wearable tai security/privacy -Aineisto käsittelee kokemuksia

Erilaisia hakusanoja ja -lausekkeita käyttäen tehtiin useita koehakuja eri tietokantoihin sekä suomeksi että englanniksi tavoitteena riittävän kattava hakutulos. Aihetta on tutkittu viime vuosina paljon, hakutulosten suuren määrän vuoksi käytettiin Metropolian kirjaston informaatikkoteknikkojen apua hakulausekkeen ja rajausten muodostamisessa. Hakukielenä on englanti, koska koehauissa suomenkielisiä tuloksia oli vähän. Kirjallisuuslähteiksi tulosten määrän rajaamiseksi valittiin vertaisarvioituja julkaisuja, joista oli koko teksti saatavilla. Aineistoa ei rajattu kielen perusteella, sillä tutkimustulokset olivat kaikki englanninkielisiä. Aikarajaus ei ole käytössä koska tutkittava ilmiö on uusi, ja koehauilla vanhimmat löydetyt aineistot olivat vuodelta 2014. Lopulliseksi hakulausekkeeksi haettaessa tietoa puettavien älylaitteiden tietoturvariskeistä muodostui lauseke (wearable* OR “wearable technology” OR “wearable sensor” OR “wearable sensing device”) AND (security OR privacy). Tulosmäärän rajaamiseksi sanat wearable*, security tai privacy tuli löytyä aineiston otsikosta. Koska koehauissa Google Scholarista löytyi aiheeseen paljon artikkeleita, yli

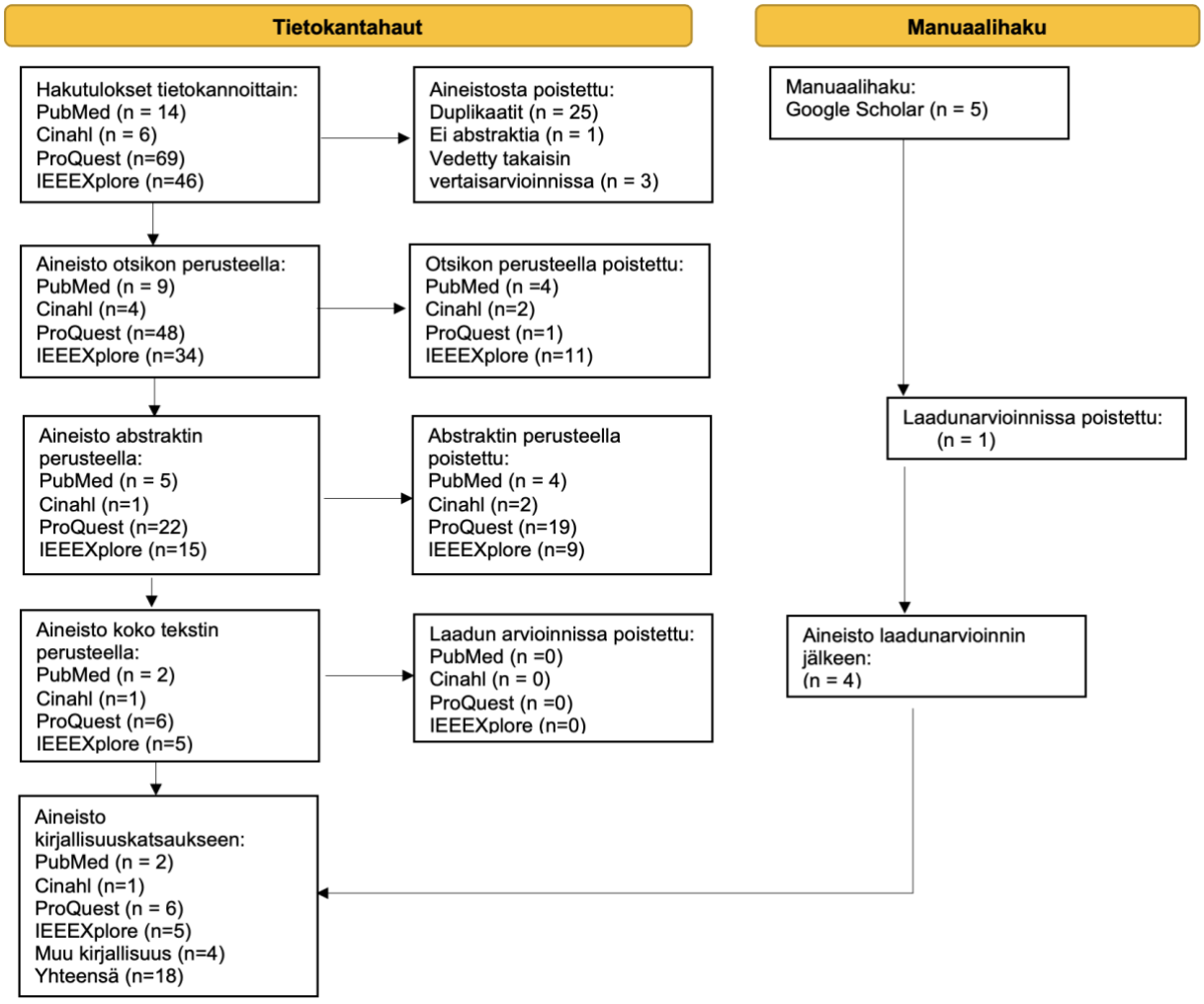
kahdeksansataatuhatta, niin haku tehtiin käsinhaulla samalla hakulausekkeella myös tästä tietokannasta. Eri tietokantoihin tehdyt haut rajauksineen kuvattu taulukossa 3.

Taulukko 3. Kirjallisuuskatsauksen haut ja rajaukset tietokannoittain

Tietokanta ja haku pvm	**Hakulauseke**	**Ei rajausta**	**Rajaus: Koko teksti Vertaisarvioitu**	**Lisärajaus: sanat wearable ja security tai privacy otsikossa**
PubMed 15.11.2023	(wearable* OR “wearable technology” OR “wearable sensor” OR “wearable sensing device”) AND (security OR privacy)	1002	948	14
Cinahl 16.11.2023	(wearable* OR “wearable technology” OR “wearable sensor” OR “wearable sensing device”) AND (security OR privacy)	323	93	6
ProQuest Central 15.11.2023	(wearable* OR “wearable technology” OR “wearable sensor” OR “wearable sensing device”) AND (security OR privacy)	331876	23808	69
Google scholar 19.11.2023	(wearable* OR “wearable technology” OR “wearable sensor” OR “wearable sensing device”) AND (security OR privacy)	-	-	Käsinhaku: 5
IEEEXplore 28.1.2024	(wearable* OR “wearable technology” OR “wearable sensor” OR “wearable sensing device”) AND (security OR privacy)	3812	270	46

Hakutulokset käytiin ensin läpi otsikkotasolla, josta valittiin artikkelit, jotka täyttivät sisäänotto- ja poissulkukriteerit ja vastasivat tutkimuskysymykseen. Seuraava valinta suoritettiin tiivistelmän perusteella ja viimeinen vaihe aineiston valinnassa oli lukea koko teksti. Katsaukseen valittiin tietokannoista ne artikkelit ja tutkimukset, jotka koko tekstin perusteella vastasivat tutkimuskysymykseen, yhteensä 14 kappaletta. Koska

kartoittavassa katsauksessa ei ole tarpeen rajoittaa mukaan otettavien tutkimusten asetelmaa vaan tietoa pyritään etsimään laajasti eri lähteistä järjestelmällistä hakustrategiaa käyttäen, mukaan otettiin myös haku harmaasta kirjallisuudesta. Harmaan kirjallisuuden haku tehtiin samalla hakulausekkeella Google Scholarista, josta mukaan katsaukseen otettiin manuaalisella valinnalla 4 artikkelia tai tutkimusta. Haun etenemisestä tehtiin Prisma-kaavio, Kuva 2.



Kuva 3. Kaavio aineiston valinnasta soveltaen Prisma Flow diagrammia. (Page ym. 2020.)

Lopulliseksi aineistoksi valittiin kahdeksantoista artikkelia, joista tietokantahauista neljätoista ja Google Scholarista neljä. Aineisto esitetään taulukossa Kirjallisuuskatsaukseen valittu aineisto Taulukko 4, Liite 1.

5.3 Aineiston laadunarvio

Katsaukseen valittujen artikkelien laadunarvioinnilla pyritään parantamaan kirjallisuuskatsauksen luotettavuutta, mutta Scoping katsauksessa tätä ei edellytetä. Scoping katsauksessa pyritään kartoittamaan laajalti olemassa olevien tutkimusten ja julkaisujen kirjoa kyseisellä aihealueella julkaisujen laadunarvioinnin sijasta. (Peters ym. 2020.) Tässä opinnäytetyössä päätettiin suorittaa aineistolle laadunarviointi luotettavuuden lisäämiseksi, sillä tutkimusalue on uusi ja julkaisujen laatu vaihtelee. Laadunarvioinnin merkitys korostui työtä tehdessä, kun havaittiin kuuden alkuperäiseen aineistoon valitun artikkelin poistuneen tietokannasta. Poistoista osan kerrottiin poistuneen johtuen huomatuista epäkohdista tai epäselvyyksistä vertaisarvioinneissa, vaikka julkaisut olivat vertaisarvioituja. Tämä nosti esiin laadun tärkeyden erityisesti uudella tutkimusalalla ja vahvistaa, kuinka tärkeää on kiinnittää huomiota artikkelien laatuun, vaikka ne ovat alun perin läpäisseet vertaisarvioinnin.

Tämän kirjallisuuskatsauksen aineiston valinnan laadun arvioinnissa käytettiin Hotuksen (Hoitotyöntutkimussäätiö) suomentamaa tutkimusten arviointikriteeristöä, jonka on kehittänyt JBI (The Johanna Briggs Collaboration). Tämä kriteeristö koostuu erilaisien tarkistuslistojen mukaan riippuen siitä, millaista tutkimusta arvioidaan. (Hotus.) Tässä opinnäytetyössä käytettiin seuraavia JBI:n tarkistuslistoja; järjestelmällinen katsaus, asiantuntijoiden näkemys ja narratiivinen teksti sekä poikkileikkaustutkimus (Hotus). Arvioinnissa käytetyt tarkistuslistat löytyvät Liite 2; Aineiston luotettavuuden arvioinnissa käytetyt JBI tarkistuslistat. Aineiston laadunarvioinnissa hylättiin 1 katsaus pistemäärällä 4/11, mikä on alle Hotuksen suosittaman 50%:n. Arvioinnin jälkeen katsaukseen valittiin 18 artikkelia.

5.4 Aineiston analyysi sisällönanalyysillä

Scoping katsauksille on ominaista, että tulokset voidaan analysoida ja esittää monin eri tavoin. Scoping katsausta tehdessä voidaan valita tuloksia, tarkoituksena löytää tietoa katsauksessa mukana olevista lähteistä ja kartoittaa niitä kuvailevasti. Scoping kirjallisuuskatsauksessa aineiston analysointimenetelmän valinta suoritetaan katsauksen tarkoituksen sekä tekijän oman harkinnan mukaan. Tärkein asia scoping katsauksen analyysin kannalta on, että tutkijat toimivat läpinäkyvästi ja selkeästi raportoivat mahdolliset analyysit. (Peters ym. 2020.)

Aineiston analyysimenetelmäksi tässä opinnäytetyössä valittiin teemoittelu. Teemoittelu on yksi laadullisen tutkimuksen sisällönanalyysin perusmenetelmistä, jossa tutkimusaineistosta pyritään keskeisiä aihepiirejä eli teemoja tunnistamaan, organisoimaan ja kategorisoimaan. (Jyväskylän yliopiston Koppa 2016.) Teemoittelu voidaan tehdä kahdella eri tavalla, joko ennalta määriteltyjen teemojen mukaan tai aineistosta esiin nousevien teemojen mukaan (Peters ym 2020). Tässä opinnäytetyössä teemoittelu tehdään aineistosta esiin nousevien teemojen mukaan. Aineistolähtöinen laadullinen sisällönanalyysi on kolmivaiheinen prosessi koostuen aineiston pelkistämisestä (redusoinnista), aineiston ryhmittelystä (klusteroinnista) ja teoreettisten käsitteiden luomisesta (abstrahoinnista). (Peters ym. 2020.) Teemoittelu aloitetaan aineiston useampaan kertaan läpikäymisellä, jossa etsitään toistuvia kuvioita ja käsitteitä. Aineiston sisältö jaetaan ryhmiin, vertaillaan ja muodostetaan luokkia, teemoja tai kategorioita jotka nimetään. Lopuksi muodostetut luokat, teemat tai kategoriat nimetään eli käsitteellistetään (abstrahointi). Saatujen tietojen tulee olla linjassa tutkimuskysymyksen ja tavoitteiden kanssa. (Peters ym. 2020: 2124; Arksey & O´Malley 2005: 26–27.)

Teemoittelu aloitettiin perehtymällä katsaukseen valittuun aineistoon lukemalla se huolellisesti useaan kertaan läpi. Aineistosta etsittiin yhtäläisyyksiä, yhteisiä asiasanoja ja tutkimuskysymystä käsitteleviä ilmauksia alkuperäisessä muodossa. Aineistossa toistuu tietoturvariskien luokittelu usealla eri tavalla sen mukaan, missä kohtaa tiedonkeruu- ja siirtoprosessia riski on. Näitä ovat muun muassa käsittely, tallennus ja siirto (Datta & Namin & Chatterjee 2018; Mills & Watson & Leyland & Kietzmann 2016), sekä laitteisto-, ohjelmisto- ja verkkouhat (Ioannidou & Sklavos 2021) tai tietojen keräämiseen, tietojen käsittelyyn, tietojen levittämiseen ja tunkeutumiseen liittyvät uhat (Nisonen 2012). Teemoittelu eteni tässä opinnäytetyössä ryhmittelemällä yhtäläisyydet, sanat ja ilmaukset ja aineistosta nousi esiin 6 pääryhmää, jotka nimettiin sisältölähtöisesti. Tästä aineistosta esiin nousseet teemat esitetään taulukossa 4.

Taulukko 4. Tuloksissa esiin nousseet teemat

Aineistosta nousseet ilmaisut	Teemat
-Tietosuojan periaatteet ja kehykset -Sijaintitietoja voidaan edelleen tunnistaa ja deanonymisoida, vaikka ne olisivat alun perin suojattu -Tietojen tallennus paikallisesti ilman salausta -Yritykset myyvät käyttäjätietoja kolmansille osapuolille ilman käyttäjän suostumusta	Tietosuoja ja yksityisyyden hallinta

Aineistosta nousseet ilmaisut	Teemat
-Lähes kaikki palvelut väittivät omistavansa käyttäjän terveystiedot -Anonymiteetin haasteet ja riskit -Tietojen keräämiseen, käsittelyyn ja jakamiseen liittyvät riskit -Yksityisyyden suojaaminen terveys- ja muun tiedon keräämisessä	
-Puettavien älylaitteiden tietoturvariskit -Heikko tietoturva, tietomurto; arkaluontoisten tietojen vaarantaminen, anastaminen, tuhoaminen tai muuttaminen -Riski: haittaohjelmat avoimien Bluetooth-porttien kautta -Vahvojen salasanojen ja tunnistautumisen puute -Sisäisen datan varastointi: Kaikki kerätty data säilytettiin laitteessa ja hyökkääjät voisivat päästä siihen käsiksi	Turvallisuus ja haavoittuvuudet
-Tietoturvastrategiat puettavissa älylaitteissa -Sijaintitietoja voidaan edelleen tunnistaa ja deanonymisoida, vaikka ne olisivat alun perin suojattu -Ne olivat haavoittuvia tehtyjä hyökkäyksiä vastaan, eikä niissä ollut riittävää suojaa salauksen ja tunnistautumisen varmistamiseksi -Liitettävyys-, käsittely-, mediaseuranta- ja tallennustilan hallintaongelmat linkittämisen ongelmat -Puettavan älylaitteen kautta päästiin käyttäjän Google Maps-haun tuloksiin ja käyttäjän sijainti haun aikana saatiin selville -Deanonymisoinnin havaitseminen ja estäminen	Teknologiset ratkaisut ja menetelmät
-Tietoturvan ja yksityisyyden lainsäädäntö -Juridiset haasteet ja sääntely eri maissa -Datanjakosopimukset ja omistusoikeus terveystietoihin -Maakohtaisten lakien ja säädösten yhtenäistäminen -Voimassa oleva lainsäädäntö, kuten HIPAA, ei koske näitä laitteita eikä niiden keräämiä terveystietoja -Standardoinnin puute	Säädökset ja oikeudelliset kysymykset
-Käyttäjien turvallisuuskäyttäytyminen; heidän tekemät luotettavuuteen liittyvät päätökset -Käyttäjien tietämättömyys riskeistä -Käyttäjän keräämää tietoa tulee kohdella yksityisenä ja olla saatavilla vain valtuutettujen henkilöiden tai yritysten käyttöön -Käyttäjien roolin kasvattaminen mm. kaksivaiheisen tunnistuksen käyttöönotolla -Joissakin puettavissa laitteissa on antureita, jotka eivät ainoastaan kerää tietoja käyttäjästä vaan myös käyttäjän ympäristöstä -Käyttäjien mahdollisuus hallita ja suojata tietojaan	Käyttäjien rooli ja tietoisuus
-Laitevalmistajien vastuu tietoturvan ja yksityisyyden suojasta -Kaikilla neljällä protokollalla on turvallisuusongelmia -Kehittäjät eivät aseta turvallisuutta ja yksityisyyttä etusijalle -Kehittäjien rooli turvallisuuden ja yksityisyyden etusijalle asettamisessa -Standardoinnin ja tietoturvaominaisuuksien merkitys -Kontekstin yksityisyydellä tarkoitetaan ongelmaa, jossa pilvipalveluntarjoajan kanssa jaetuista anturitiedoista voidaan tehdä päätelmiä käyttäjän kontekstista ja toimista -Vahvojen salasanojen ja tunnistautumisen puute	Laitevalmistajien ja kehittäjien vastuu

6 Tulokset

Kirjallisuuskatsauksen tulokset esitellään aineistosta nousseiden teemojen mukaan. Teemoja ovat: tietosuoja ja yksityisyyden hallinta, turvallisuus ja haavoittuvuudet, teknologiset ratkaisut ja menetelmät, säädökset ja oikeudelliset kysymykset, käyttäjien rooli ja tietoisuus sekä laitevalmistajien ja kehittäjien vastuu.

6.1 Tietosuoja ja yksityisyyden hallinta puettavissa älylaitteissa

Puettavien älylaitteiden käyttöön liittyy merkittäviä haasteita ja riskejä. Puettavien laitteiden, kuten älykellojen ja kuntoilulaitteiden käytön huomattava lisääntyminen on tuonut esille tietosuojan ja yksityisyyden puutteita. (Vaishnavi & Sahana & Guruprasad 2023.) Aiemmin on tarkasteltu lääkinnällisten laitteiden yksityisyyskysymyksiä, kuluttajien puettavien älylaitteiden yksityisyysriskejä on selvitetty huomattavasti vähemmän (Shukur & Fatlawi 2022). Laitteiden yleistyminen parantaa hyvinvointia herättäen kuitenkin huolta yksilöiden henkilötietojen yksityisyydensuojasta, sillä niiden avulla voidaan seurata käyttäjien toimintaa internetissä (Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad 2023). Myös yritykset ovat alkaneet tiedostaa työntekijöiden käyttämien älylaitteiden muodostaman riskin arkaluontoisten tietojen vuotamiselle ja tietoturvauhille yrityksen verkkoon (Mills & Watson & Layland & Kietzmann 2016).

Älypuhelinten sovellukset pyytävät laajoja käyttöoikeuksia, jotka eivät ole perusteltuja tietosuojakäytäntöjen valossa. Tutkituista sovelluksista neljä viidestä tekee tietopyyntöjä, jotka koskevat äänen tallentamista mikrofonilla, puheluiden soittamista ja vastaanottamista sekä viestien lukemista ja lähettämistä. Vaikka kaikkien sovellusten tietosuojakäytännöissä tietojen kerääminen käyttökokemuksen parantamiseksi on selvästi mainittu, syyt kameran hallintaan, äänitallennukseen tai jopa tekstiviestien käyttöön ja puheluihin liittyvien oikeuksien myöntämiseen ovat edelleen epämääräisiä. (Ioannidou & Sklavos 2021.)

Jotkut puettavat älylaitteet ovat varustettu kameroilla, jotka voivat tallentaa ohikulkijoiden toimintaa ilman heidän ennakkosuostumustaan tai tietoisuuttaan, herättäen huolta jatkuvasta tallennuksesta (Shukur & Fatlawi 2022; Chin & Singh 2016). Ihmiset ottavat videoita, valokuvia tai äänitallenteita tehdessään päivittäisiä askareitaan ja julkaisevat ne verkossa aiheuttaen yksityisyysongelmia sekä viattomille

sivullisille että laitteen käyttäjälle. Näennäisen harmittomien laitteiden tallenteet voivat paljastaa sijainnin ja muita arkaluonteisia tietoja, kuten kuvan pankkiautomaatista, kun sivullinen on suorittamassa maksutapahtumia. (Datta & Namin & Chatterjee 2018.) Tiedot tallennetaan paikallisesti ilman salausta (Chin & Singh 2016). Erityisesti laitteiden keräämät herkät käyttäjätiedot, kuten kunto- ja terveysmittaukset, ovat alttiita väärinkäytöksille. Esimerkiksi vuonna 2019 havaittiin, että tietyt Kiinassa valmistetut älykellot mahdollistivat hakkerien pääsyn kuuntelemaan ja muokkaamaan yksityisiä keskusteluja. (Vaishnavi & Sahana & Guruprasad 2023). Tämä ongelma on osittain seurausta siitä, että käyttäjätietojen omistajuus on usein epäselvä ja laitteet voivat tallentaa ja jakaa tietoja ilman käyttäjien suostumusta (Cusack & Antony & Ward & Mody 2017). Laitteiden toissijaiset laitemoduulit eivät vaadi erityisiä käyttäjän oikeuksia, kuten gyroskooppi ja kiihtyvyysmittarit, jolloin näitä voidaan käyttää välineenä keskustelujen salakuunteluun ilman suostumusta tai yhdistettynä paljastamaan herkkiä terveystiloja (Ioannidou & Sklavos 2021).

Tietosuojan näkökulmasta erityisen ongelmallista on käyttäjätietojen omistajuuden epäselvyys ja puettavat laitteet voivatkin tallentaa ja jakaa tietoja kaupallisiin tarkoituksiin ilman käyttäjien suostumusta (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Ioannidou & Sklavos 2021; Mills & Watson & Leyland & Kietzmann 2016; Zhou & Piramuthu 2014). Puettavat älylaitteet ovat yhä henkilökohtaisempia yhdistyessään käyttäjän muihin tietojärjestelmiin, kuten älypuhelimiin ja tietokoneisiin, jotka voivat toimia portteina laajempiin laitteistossa säilytettyihin tietoihin (Mills & Watson & Leyland & Kietzmann 2016). Käyttäjien odotukset tietojen omistajuudesta ovat ristiriidassa yritysten käytäntöjen kanssa, joissa puettavien laitteiden, ohjelmistojen ja pilvipalveluiden tarjoajat vaativat omistusoikeutta kerättyihin tietoihin (Cusack & Antony & Ward & Mody 2017; Mills & Watson & Leyland & Kietzmann 2016).

Mainonta ja markkinointistrategiat hyödyntävät kerättyjä henkilötietoja rakentaen ja paljastaen henkilöllisyyksiä kolmansille osapuolille ilman käyttäjän tietämystä tai suostumusta. Tämä saattaa sisältää pääsyn tiettyihin laitteen toimintoihin, kuten puheluihin, tekstiviestien lukemiseen ja GPS-seurantaan, sekä laitteen sisältämien tietojen, valokuvien, videoiden ja yhteystietoluettelon käyttämiseen. Profiloinnissa käytetään runsaasti arkaluonteisia henkilötietoja, kuten puhelinnumeroa, osoitetta, pankkitiliä, IP-, ALV- ja henkilökortin numeroita, jotka täydennetään käyttäytymistiedoilla, kuluttajien mieltymyksillä, poliittisilla vakaumuksilla, alueellisilla ja

ajallisilla valinnoilla tai jopa biometrisillä tai biokemiallisilla ominaisuuksilla. Henkilötiedot ovat digitaalisessa muodossa helposti jälleenmyytävä tuote. Yhden laajalti käytetyn toiminnan seurantasovelluksen havaittiin jakavan valtavan määrän tietoa laitteesta ja käyttäjästä 76 eri kolmannelle osapuolelle. (Ioannidou & Sklavos 2021.) Tämä kompleksisuus luo haasteita, kun pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus (Cusack & Antony & Ward & Mody 2017; Mills & Watson & Leyland & Kietzmann 2016).

Käyttäjien tietoisuutta on tärkeää lisätä heidän tietojensa käyttötarkoituksista ja käsittelystä. GDPR-aikakaudella henkilötietojen käsittelyn ja yksityisyyden suojan merkitys korostuu. (Ioannidou & Sklavos 2021.) Yhteenliittyvyys luo monimutkaisia haasteita tiedon omistajuuden osalta (Cusack & Antony & Ward & Mody 2017). Siitä huolimatta useat yritykset jatkavat palveluiden tarjoamista epämääräisten käytäntöjen mukaisesti (Ioannidou & Sklavos 2021).

Tietojen vaarantuminen, muokkaus ja mahdollisuus kuunteluun ovat herättäneet huolta. Ilman asianmukaisia tietosuojasäädöksiä arkaluontoiset käyttäjätiedot ovat alttiita väärinkäytöille. (Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad 2023.) Vaikka laitteen fyysinen kompromissointi on uhkatekijä, varsinaiset riskit kohdistuvat usein käyttäjän tietojen suojaan eikä niinkään fyysiseen hyvinvointiin. Yksinkertainenkin hakkerointi voi johtaa siihen, että käyttäjä vaarantaa kaikki tietonsa, ne varastetaan, tuhotaan tai niihin tehdään muutoksia. (Ioannidou & Sklavos 2021; Mills & Watson & Leyland & Kietzmann 2016.)

Tietoturvasuunnittelun periaatteet edellyttävät tiedon luottamuksellisuutta, eheyttä ja saatavuutta, mutta BLE-kuntorannekkeet ja terveyslaitteet keräävät runsaasti henkilökohtaista tietoa ja niiden yhteydenmuodostus on toteutettu ilman asianmukaista todennusta (Barua & Alamin & Hossain & Hossain 2022; Peker & Bello & Perez 2022). Tietojen kerääminen ja jakaminen tapahtuu usein ilman käyttäjän suostumusta ja laitteiden kautta saatetaan paljastaa erittäin arkaluontoisia tietoja, kuten käyttäjän syntymäaika ja sosiaaliturvatunnus. Heikon todentamisen ja salauksen puutteen kautta laitteet paljastavat käyttäjän sijainnin. (Barua & Alamin & Hossain & Hossain 2022; Chin & Singh 2016; Mills & Watson & Layland & Kietzmann 2016; Zhou & Piramuthu 2014.) Suunnitteluvirhe vähän virtaa käyttävissä Bluetooth-laitteissa paljasti yksityisyysongelmia, kuten sormenjälkitunnistushyökkäyksen (Barua & Alamin & Hossain & Hossain 2022). HCI Snoop Log -ominaisuus Bluetooth-protokollassa

paljastaa tekstinä viestien lähettäjän henkilöllisyyden (Cusack & Antony & Ward & Mody 2017).

Google Glass, Fitbit ja Samsung- älykello olivat alttiita tietoturvaongelmille, sillä niiden käyttö vaatii pariliitoksen esimerkiksi älypuhelimen kanssa useimpien toimintojen suorittamiseksi. Tämä pariliitos toteutetaan usein suojaamattoman BLE:n kautta. (Chin & Singh 2016.) Analysoidessa kahta puettavaa älylaitetta ja yhtä näppäimistöä, huomattiin etteivät BLE-standardin mukaiset turvamekanismit toteutuneet. Laitteita seurattiin, käyttäjätiedot vaarantuivat ja lähetetyt tiedot vuotivat. Yksi laitteista ei lopettanut laitetietojen lähettämistä yhteyden muodostamisen jälkeen. Kaikissa kaapatuissa tiedoissa jatkui mainospakettien lähettäminen edesauttaen laitteen helppoa jäljittämistä. Laite vuoti anturidataa mainospakettien kautta, jotka sisälsivät syketietoja ja mainospaketit lähetettiin aina näkyvästi ilman salausta. Data saatettiin myös kerätä kolmannen osapuolen laitteella rikkoen käyttäjän yksityisyyttä. (Peker & Bello & Perez 2022.)

Pääsy laitetietoihin, kuten sijaintiin, on perusteltua kaikille kuntoseurantasovelluksille tarpeella käyttäjälle toimitettujen tietojen tallentamiseen ja optimointiin (Ioannidou & Sklavos 2021). Oikeus seurata henkilöä kuntoseurantalaitteen käytön perusteella on melko vakavaa, varsinkin kun ne voidaan toteuttaa ilman että käyttäjä tietää siitä (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Zhou & Piramuthu 2014). Puettavaa laitetta voidaan myös käyttää käyttäjien paikantamiseen aikomuksena vahingoittaa heitä tai heidän laitteitaan tai murtautua heidän omaisuuteensa (Mills & Watson & Leyland & Kietzmann 2016). Käyttäjän arkaluonteiset tiedot on suojattava, jotta hänen elintapansa eivät paljastu (Ioannidou & Sklavos, 2021). Yhdistämällä fysiologiset mittaustulokset, aika, paikka ja toiminto voidaan tehdä päätelmiä käyttäjästä (Datta & Namin & Chatterjee 2018). Lisäksi näiden mittausten perusteella, esimerkiksi vain käsittelemällä älypuhelimen kiihtyvyysanturin ja gyroskoopin signaalien keräämiä kävelytietoja, on mahdollista tunnistaa kohdekäyttäjä (Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021).

Tietoturva-analyysin perusteella Google Glass, Fitbit ja Samsung-älykello ovat kaikki alttiita erilaisille tietoturvaongelmille. Google Glass ei tarjoa riittävän turvallista PIN-koodijärjestelmää. Laitteen silmienseurantateknologia ja mahdollisuus tallentaa kuvia ja videoita ilman käyttäjän suostumusta loukkaavat käyttäjän yksityisyyttä. Fitbit-laitteissa havaittiin puutteellinen todentaminen, mikä mahdollistaa tietojen vapaan liikkumisen

ilman käyttäjän tietämystä. Tämä avaa ovet erilaisille hyökkäyksille, kuten datainjektio- ja palvelunestohyökkäys. Samsung Smartwatch -älykellojen tutkimuksessa paljastui merkittäviä haavoittuvuuksia, kuten heikko todentaminen ja salauksen puute sekä suojaamaton verkko. Näiden laitteiden kautta käyttäjän sijainti voidaan jäljittää, lisäten entisestään tietoturvariskejä. (Chin & Singh 2016.) Google Glass voi tallentaa sivullisia ja heidän toimintaansa ilman suostumusta. Yksityisyyden loukkaukset ulottuvat myös fysiologisiin mittaustuloksiin, joiden avulla voidaan tunnistaa yksilöitä. Käyttäjän tietojen uudelleentunnistamisen riski on korkea, sillä tutkimuksessa havaittiin hyvin pienten datamäärien, kuten 2 sekunnin EEG-tallennuksen tai 50 sekunnin kiihtyvyys- ja gyroskooppidatan voivan tunnistaa yksilön suurella tarkkuudella. Tämä osoittaa, että hyvin pienet datamäärät voivat aiheuttaa suuria yksityisyyden riskejä. (Chikwetu ym. 2023.)

6.2 Turvallisuushaasteet ja haavoittuvuudet puettavien älylaitteiden käytössä

Riski tietovuotoihin on huomattava, koska puettavat älylaitteet on suunniteltu olemaan jatkuvasti yhteydessä verkkoon (Chikwetu ym. 2023; Mills & Watson & Leyland & Kietzmann 2016). Sensoridataa jaettaessa uudelleentunnistamisen riski voidaan minimoida muttei täysin eliminoida. Pelkkä tunnistetietojen pidättäminen ja julkisista tietovarastoista poistaminen ei ole riittävää yksityisyyden turvaamiseksi. (Chikwetu ym. 2023.) Yksityisyysriskit, jotka liittyvät tietojen keräämiseen puettavien älylaitteiden kautta, ovat merkittäviä. Käyttäjä voi jakaa muun muassa sydämensä syketiedot, mutta samat tiedot kerätään ja lähetetään sovellukselle jatkuvasti, riippumatta käyttäjän tahdosta. (Langley 2015.)

Monet organisaatiot ovat vastustaneet puettavien älylaitteiden käyttöä työpaikoilla; työntekijät pelkäävät työnantajan seurantaa, laitteiden käyttö turvallisuuskriittisissä ympäristöissä kuten öljy- ja kaasuteollisuudessa herättää huolta, laitteet voivat aiheuttaa häiriöitä tai häiriötekijöitä ja ne saattavat tallentaa arkaluonteisia tietoja työpaikalla aiheuttaen pelkoa tietovuodoista, sillä käyttäjä voi kerätä, prosessoida sekä jakaa dataa eteenpäin (Datta & Namin & Chatterjee 2018).

Laitteiden hallinta voidaan menettää haittaohjelmien tai tietoturvaloukkausten seurauksena, jolloin syntyy riski arkaluontoisten tietojen vuotamiselle, vaarantumiselle, anastamiselle, tuhoamiselle tai muuttamiselle. Merkittävä riski on myös vahvojen

salasanojen puute. Käyttäjää voidaan johtaa harhaan virheellisillä tiedoilla tai hänen fyysistä turvallisuuttansa vaarantaa laitteita vahingoittamalla tai hakkereiden häiritessä niiden toimintaa. (Cai & Venkatasubramanian 2018; Mills & Watson & Leyland & Kietzmann 2016; Vaishnavi & Sahana & Guruprasad 2023.) Myös flash-muisti voidaan sulkea, mikä tekee emolevyn käynnistämisen mahdottomaksi. Järjestelmäkutsuja pystytään sieppaamaan ja estämään lukeminen ja kirjoittaminen tiettyihin NAND-flashin osioihin. Tällöin estetään tiettyjen tiedostojen poistaminen päivityksestä huolimatta ja laitteeseen asennettuihin ohjelmistoihin jää takaovi hyökkääjien käyttöön. (Arias & Wurm & Hoang & Jin 2016.) Laitteisto- ja ohjelmistotroijalaisten asentaminen on mahdollista vaarantaen laitteiden toiminnallisuuden vuotaen keskeisiä tietoja hyökkääjälle, aiheuttaen laitteen toimimisen määriteltyjen parametrien ulkopuolella tai tekemällä laitteesta toimimattoman. Troijalainen voi mahdollistaa etähyökkäykset ja laajemman verkkovalvonnan, mukaan lukien liikenteen uudelleenohjauksen ja laajempien hyökkäysten käynnistämisen. Laitteistotroijalaiset voivat jäädä huomaamatta normaaleissa testausmenetelmissä ja niiden havaitseminen vaatii kalliita erikoistestejä. (Arias & Wurm & Hoang & Jin 2016; Mills & Watson & Leyland & Kietzmann 2016.)

Turvallisuusuhka, jossa tietoturvaloukkaus vaarantaa sekä käyttäjän että laitteen fyysiset ominaisuudet, on todellinen sillä hakkerit voivat estää laitteiden toiminnan vahingoittamalla sitä tai kytkemällä ne etänä pois päältä (Mills & Watson & Leyland & Kietzmann 2016; Vaishnavi & Sahana & Guruprasad 2023). Esimerkkeinä mainitaan äkkinäinen voimakkaan ulkotukirangan (powered exoskeleton) sammuminen, älykellon aiheuttama sähköisku haptisen laitteiston kautta tai se, että kirurgisen älykäsineen hienous ja tarkkuus voitaisiin kytkeä pois päältä kesken leikkauksen tai sen tarkkuutta voidaan muuttaa tavalla, joka saa kirurgin tekemään virheitä ja vaarantaa potilaan. Harhauttaminen ja virheelliset terveyteen liittyvät tiedot, esimerkiksi älykuulokkeisiin syötettävää dataa vääristelemällä, vaikuttavat käyttäjän hyvinvointiin ja päätöksentekoon terveydestään. Rikkomalla laitteen tietoturvaa, kolmas osapuoli voi oppia paljon käyttäjän käyttäytymisestä pahantahtoisissa tarkoituksissa. Vaihtoehtoisesti käyttäjän laitteessa olevia tietoja voidaan manipuloida välittämään väärää tietoa henkilön käytöksestä (Mills & Watson & Leyland & Kietzmann 2016; Vaishnavi & Sahana & Guruprasad 2023), esimerkiksi siitä, että hän noudattaa lääketieteellistä hoito-ohjelmaa, vaikka ei noudattanut sitä, tai saada lääkäri määräämään lisälääkitystä, kun potilas ei sitä tarvinnut (Mills & Watson & Leyland & Kietzmann 2016).

Geotiedot mahdollistavat haitalliset hyökkäykset sijainnin yksityisyyttä vastaan, kuten sijainnin ennustaminen toimintohistorian avulla, kaupunkitietoon perustuva kaupunkiennustus ja kaupunkiennuste ilman ennakkotietoa (Ioannidou & Sklavos 2021; Okonkwo & Awolusi & Nnaji 2022). Tietoturvariskejä ei voida pitää pelkästään teoreettisina, sillä ne saattavat johtaa konkreettisiin fyysisiin, maineeseen liittyviin ja taloudellisiin seurauksiin (Cusack & Antony & Ward & Mody 2017; Vaishnavi & Sahana & Guruprasad 2023). Esimerkiksi vuoden 2020 lunnasohjelmaisku älykellojen valmistajaa Garminia vastaan aiheutti palvelunestohyökkäyksen ja datan vuotamisen, korostaen tietoturvaongelmien jatkuvan valvonnan ja turvallisuusprotokollien päivitystarvetta (Vaishnavi & Sahana & Guruprasad 2023).

Hyökkääjä voi toistuvasti lähettää puettavan älylaitteen tunnistetta verkkopalvelimelle ja hakea etukäteen sarjan vastauksia. Vastaukset seurantalaitteelle toistamalla saadaan seurantalaite uskomaan, että se kommunikoi verkkopalvelimen kanssa. Tämä menetelmä mahdollistaa verkkopalvelimen aseman matkimisen seurantalaitteen näkökulmasta. Tunkeutuja voi myös toteuttaa desynkronointihyökkäyksen estämällä toistuvasti viestin kulun verkkopalvelimelta puettavaan älylaitteeseen. Tunnuksissa esiintyvä epäjohdonmukaisuus näiden välillä johtaa niiden pysyvään epäsynkronointiin. Samankaltainen hyökkäys voidaan toteuttaa myös estämällä viesti laitteesta verkkopalvelimelle. (Zhou & Piramuthu 2014.)

Tietoturva-analyysin tulokset puettavien älylaitteiden turvallisuudesta ja haavoittuvuuksista ovat huolestuttavia. FitLock-järjestelmässä olevat haavoittuvuudet sallivat varastetun kuntoiluun käytetyn puettavan älylaitteen liittämisen toiseen verkkotiliin ilman asianmukaista tunnistautumista. (Zhou & Piramuthu 2014.) Nest termostaatin analyysi paljasti debug-rajapintojen ja heikkojen kryptografisten toteutusten luomat uhat. Nike+ Fuelband -laitteen STM32-mikroprosessorin suojausominaisuuksia ei ole hyödynnetty, jolloin hyökkääjät voivat vapaasti muokata laitteen flash-muistin sisältöä ja ohittaa suojausmekanismit. (Arias & Wurm & Hoang & Jin 2016.) Laitteiden etäpäivityksille suunniteltu kryptografia osoittautuu monimutkaiseksi tehtäväksi, jossa virheet toteutuksessa voivat johtaa vakaviin tietoturvariskeihin. Esimerkiksi Belkin WeMo Home Automation -laitteen tapauksessa SSL:n virheellinen käyttö mahdollisti haittaohjelmiston etäasentamisen, heikentäen laitteen turvallisuutta merkittävästi. (Arias & Wurm & Hoang & Jin 2016.) Vahvojen kryptografisten protokollien puute ja standardoitujen turvallisuusprotokollien heikkoudet ovat herättäneet kysymyksiä IoT-laitteiden turvallisuuden riittävyydestä (Toorani 2015).

Laitteen standardi USB-liitäntä mahdollistaa uuden laiteohjelmiston kirjoittamisen (Arias & Wurm & Hoang & Jin 2016). Tapaustutkimuksessa huomattiin, että Samsung Gear S3: sen kautta päästiin käyttäjän Google Maps-haun tuloksiin ja käyttäjän sijainti haun aikana saatiin selville. Sijaintitietoja voidaan edelleen tunnistaa ja deanonymisoida, vaikka ne olisivat alun perin suojattu. (Park & Riha & Yoon & Lee 2021.) Puettavien älylaitteiden integrointi IoT-verkkoihin lisää verkkopohjaisten hyökkäysten mahdollisuutta (Vaishnavi & Sahana & Guruprasad 2023).

Nest Thermostaatin piirilevyn analyysi paljastaa, että sys boot-liittimen näkyvyys ja tyhjä otsake mahdollistavat prosessorin uudelleenkäynnistyksen ulkoisista liitännöistä, kuten USB:stä tai UART3:sta, ja antavat mahdollisuuden käyttäjän koodin syöttämiseen laitteeseen. Lisäksi termostaatin tehdas asetuksiin palautus voi johtaa vastaavaan tulokseen. Koska ROM ei tarkista syötettävää koodia, tämä avaa mahdollisuuden koodin rajoittamattomaan käyttöön, kunhan laitteen havaitsemisen ja ohjelmoinnin ajoitusikkunat ovat oikein asetettu. Suljetun lähdekoodin järjestelmissä hyökkääjän on vaikeampi löytää virheitä ohjelmistosta, kun taas avoimen lähdekoodin ohjelmistoissa potentiaaliset hyökkäysvektorit löytyvät helpommin. Lisäksi päivitysten vastaanottaminen salaamattoman yhteyden kautta ja päivityskuvien allekirjoitusten manipulointi on mahdollista, jos laite on vaarantunut. IoT-laitteiden suunnitteluun liittyvät turvallisuus- ja haavoittuvuuskysymykset ovat monimutkaisia. Esimerkiksi, avoimen ja suljetun lähdekoodin ohjelmistojen sekä laitteiston suunnittelun valinnat voivat vaikuttaa laitteen alttiuteen hyökkäyksille. Nest Termostaatin esimerkki paljastaa, miten debug-rajapinnat ja heikot kryptografiset toteutukset tarjoavat mahdollisuuksia laitteiston manipulointiin ja luvattomaan pääsyyn, korostaen tarvetta jatkuvalle turvallisuuden tarkastelulle ja päivityksille. Laitteen rikosteknisessä lisäanalyysissä havaittiin, että kaikki lokitetut tiedot oli tallennettu ja että ne oli mahdollista hakea luvattomista lähteistä. (Arias & Wurm & Hoang & Jin 2016.)

WMS, Wearable Medical Systems, eli puettavat lääkinnälliset älylaitteet keräävät arkaluontoisia tietoja käyttäjistään tehden niistä houkuttelevia kohteita hakkereille. Datan manipulointi voidaan suorittaa iskemällä langattomaan linkkiin anturin ja tukiaseman välillä tai kompromisoimalla anturin ohjelmiston tai kirjaston päivitysprosessin. Tällaiset hyökkäykset voivat johtaa kahdentyyppisiin seurauksiin; potilastietojen vuotamiseen sekä WMS-järjestelmän toimintahäiriöihin, jotka voivat vahingoittaa käyttäjää. Viime aikoina on raportoitu useista anturidatan manipulaatiohyökkäyksistä, jotka hyödyntävät langattoman verkon heikkouksia,

esimerkiksi sydämentahdistimissa ja insuliinipumpuissa. Anturit ovat alttiita sensory-channel-hyökkäyksille, jotka sekoittavat anturien signaaleja ja syöttävät virheellisiä mittausarvoja järjestelmään. Esimerkiksi vääristettyjä sydänsähkökäyriä (EKG) saadaan näyttämään hengenvaaralliset rytmihäiriöt normaaleina. (Cai & Venkatasubramanian 2018.)

Rakennusteollisuuden langattomat IoT-järjestelmät (WIoT) ovat alttiita samanlaisille tietoturvauhille kuin muidenkin alojen, koko arkkitehtuurinsa laajuudessa havaintokerroksesta sovelluskerrokseen. Nämä haavoittuvuudet voivat rikkoa tietoturvaa, vaikuttaa verkon käytettävyyteen ja vaarantaa todennuksen ja palvelujen eheyden. Tyypillisiä turvallisuusuhkia ovat tavallisten BLE-ongelmien lisäksi anturisolmuille kohdistuvat hyökkäykset, luvattomat RFID-pääsykokeilut, univajehyökkäyksen aiheuttamat häiriöt ja väärennetyt yhteydet, sekä haittaohjelmien leviäminen. Tunnistettuihin tietoturvariskeihin kuuluvat myös huijaus- ja sinkhole-hyökkäykset, joissa järjestelmään pyritään pääsemään luvattomasti käsiksi tai ohjaamaan verkkoliikennettä väärennetyillä reititystiedoilla. Näiden hyökkäysten seurauksena saattaa ilmetä tietojen vuotoja, luvaton pääsy, todennusvirheitä ja järjestelmän väärinkäyttöä, joiden seurauksena kaikki järjestelmässä käsitellyt ja tallennetut tiedot voivat vaarantua. (Okonkwo & Awolusi & Nnaji 2022.)

Puettavat älylaitteet ovat osa IoT:tä ja hauraita tekniikoita, jotka ottavat käyttöön verkon ja laitteiden haavoittuvuudet, joihin ne on kytketty (Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad 2023). Tämä tarkoittaa pääasiassa suojaamattomia Bluetooth-yhteyksiä tai Wi-Fi-verkkoja, jotka yhdistävät puettavat laitteet muuhun tekniikkaan, tyypillisesti muihin mobiililaitteisiin kuten älypuhelimiin (Mills & Watson & Leyland & Kietzmann 2016). Molemmat yhteystyypit ovat suhteellisen helppoja murtaa brute force -hyökkäyksellä (Chin & Singh, 2016; Cusack & Antony & Ward & Mody 2017; Mills & Watson & Leyland & Kietzmann 2016; Peker & Bello & Perez 2022). BLE-tietoturva kohtaa haasteita erityisesti laitepariliitosten tietoturvaongelmien vuoksi (Barua & Alamin & Hossain & Hossain 2022; Cusack & Antony & Ward & Mody 2017; Silva-Trujillo & González González & Pérez & García Villalba 2023), yleisimmät näistä ovat man-in-the-middle- hyökkäys, salakuuntelu, pakettien injektointi sekä identiteetin paljastuminen selkokielisenä (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Okonkwo & Awolusi & Nnaji 2022; Silva-Trujillo & González González & Pérez & García Villalba 2023; Vaishnavi & Sahana & Guruprasad 2023). Tietoja voidaan varastaa tai hyökkääjä voi jopa kirjoittaa yli BLE-laitteen tiedot ja aiheuttaa

odottamatonta toimintaa (Barua & Alamin & Hossain & Hossain 2022). Laitteille on mahdollista suorittaa pakotettu uudelleen paritus (Cusack & Antony & Ward & Mody 2017; Silva-Trujillo & González González & Pérez & García Villalba 2023).

Puettavat älylaitteet, kuten älykellot, kärsivät heikoista todennusmekanismeista, kiinteistä MAC-osoitteista ja salaamattomista yhteyksistä mahdollistaen luvattoman pääsyn laitteisiin (Cusack & Antony & Ward & Mody 2017; Mills & Watson & Leyland & Kietzmann 2016; Peker & Bello & Perez 2022; Silva-Trujillo & González González & Pérez & García Villalba 2023; Zhou & Piramuthu 2014), haittaohjelmista avoimien Bluetooth-porttien kautta (Cai & Venkatasubramanian 2018; Okonkwo & Awolusi & Nnaji 2022), blue print hyökkäyksistä (Cusack & Antony & Ward & Mody 2017), tietojen tahallisesta muokkauksesta (Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad, 2023), sniffing-hyökkäyksistä (Silva-Trujillo & González González & Pérez & García Villalba 2023) sekä hajautetuista palvelunestohyökkäyksistä (DDoS) (Chikwetu ym. 2023; Chin & Singh 2016; Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad, 2023).

BLE-teknologiaa hyödyntävät laitteet ovat osoittautuneet alttiiksi jäljitykselle (Cusack & Antony & Ward & Mody 2017; Peker & Bello & Perez 2022) ja phishing-hyökkäyksille (Chin & Singh 2016; Okonkwo & Awolusi & Nnaji 2022; Peker & Bello & Perez 2022). Vakavia heikkouksia on havaittu myös laiteohjelmiston päivitysprosessissa, mikä mahdollistaa laitteistotroijalaisten asentamisen (Arias & Wurm & Hoang & Jin 2016) ja salatun tiedon vuotamisen (Arias & Wurm & Hoang & Jin 2016; Barua & Alamin & Hossain & Hossain 2022; Cusack & Antony & Ward & Mody 2017; Ioannidou & Sklavos 2021; Okonkwo & Awolusi & Nnaji 2022; Peker & Bello & Perez, 2022; Vaishnavi & Sahana & Guruprasad 2023).

Google Glass, Fitbit ja Samsung Smartwatch -laitteiden havaittiin olevan alttiita Wi-Fi-kaappauksille, QR-koodihyökkäyksille sekä BLE-teknologian heikkouksille jotka voivat johtaa käyttäjän hallinnan menettämiseen ja tietojen turvallisuuden vaarantumiseen. Laitteet olivat jäljitettävissä, niissä oli heikko todennus ja salaamaton laiteohjelmisto. (Chin & Singh 2016.) Samaan tulokseen päädyttiin kahden muun älylaitteen ja yhden älynäppäimistön turvallisuusanalyysissa (Peker & Bello & Perez 2022). Esimerkiksi ihmisen fysiologisten tietojen varastaminen suojaamattomissa BLE-yhteyksissä voidaan hyödyntää toistohyökkäyksissä biometrisissä autentikointimenetelmissä. Havaittiin vaihtelevia turvallisuuden toteutustasoja, jotka osoittivat

epäjohdonmukaisuuksia laitteiden Bluetooth-toteutuksissa. Fitbit Charge vaatii PIN-koodin, jonka on oltava yhtenevä molemmissa laitteissa ennen parittamista. Tämä ei vastaa Bluetooth Special Interest Groupin (SIG) kuvailemia määritelmiä, sillä käyttäessään nelinumeroista PIN-koodia kuuden numeron sijasta se mahdollistaa arvaushyökkäyksen onnistumisen erittäin nopeasti. Fitbit Charge on helposti jäljitettävissä, sillä se ei käyttänyt osoitteen satunnaistamista. Analysoiduissa laitteissa oli haavoittuvuuksia, joita voidaan hyödyntää käyttäjien jäljittämiseen sekä yksityisen tai arkaluonteisen tiedon keräämiseen datapakettien salaamattomuuden vuoksi. (Peker & Bello & Perez 2022.) Havaintojen mukaan kaikki viisi sovellusta keräävät sijainti- ja henkilökohtaisia tunnisteita ja muodostavat yhteyden Bluetoothin kautta ilman todennusta (Ioannidou & Sklavos 2021). Äskettäin Singaporesta kotoisin oleva tutkimusryhmä kuvaili sarjan haavoittuvuuksia BLE-laitteissa, jotka he nimesivät SweynTooth-haavoittuvuuksiksi (Barua & Alamin & Hossain & Hossain 2022).

IEEE 802.15.6-standardi on kansainvälinen langattomia kehon alueverkkoja (Wireless Body Area Networks, WBAN) koskeva standardi, joka keskittyy langattomien, kehoa lähellä pidettävien laitteiden viestintäprotokolliin ja niiden turvallisuuteen. Se sisältää määräyksiä laitteiden turvallisien yhteyksien luomisesta, tietojen vaihtamisesta sekä avaintenvaihdon suorittamisesta. Standardi on suunniteltu tukemaan reaaliaikaista terveydenseurantaa suorittavia ja kuluttajaelektroniikan sovelluksia ollen kriittinen infrastruktuurin komponentti terveydenhuollossa ja henkilökohtaisessa elektroniikassa. Tutkimuksessa havaittiin standardissa olevien turvallisuusprotokollien olevan haavoittuvaisia useille hyökkäyksille suorittamalla tietoturva-analyysi ja haastamalla erilaisin hyökkäyksin neljä avaintenvaihtoprotokollaa. Kaikilla neljällä protokollalla on turvallisuusongelmia. Ne olivat haavoittuvia tehtyjä hyökkäyksiä vastaan (KCI, imitaatio, offline-sanakirja) eikä niissä ollut riittävää suojaa tunnistautumisen ja eteenpäin suuntautuvan salauksen, PFS:n (Perfect forward securityn) varmistamiseksi. Jos julkisia avaimia ei validoida, protokollat voivat olla alttiita lisähyökkäyksille, kuten invalid-curve hyökkäys, jonka avulla hyökkääjä voi paljastaa toisen osapuolen yksityisen avaimen. (Toorani 2015.)

6.3 Teknologiset ratkaisut ja menetelmät puettavien älylaitteiden tietoturvariskien mahdollistajina

Laitteen, joka on suunniteltu päivitettäväksi etänä, on kyettävä varmistamaan ladatun ohjelmakuvan eheys ja aitous (Arias & Wurm & Hoang & Jin 2016). Tämä edellyttää

usein monimutkaisten kryptografisten algoritmien käyttöä. Kryptografisen suojauksen toteuttaminen on haastavaa, kuten lukuisat ohjelmistohaavoittuvuudet ovat osoittaneet. Nämä johtuvat paitsi matemaattisista haasteista, myös toteutusvirheistä. Vahvojen salasanojen puute ja kriittiset haavoittuvuudet kryptografisissa järjestelmissä mahdollistavat laitteisiin kohdistuvat etähyökkäykset ja sallivat väärennetyn ohjelmiston asennuksen. (Arias & Wurm & Hoang & Jin 2016; Mills & Watson & Pitt & Kietzmann 2016.) Järjestelmien tulisi täyttää vaatimukset tunnistautumisessa, anonymiteetissä, salauksessa ja liikenteen seurannassa (Okonkwo & Awolusi & Nnaji 2022).

Arkaluonteisia tietoja välittävissä langattomissa järjestelmissä on yleinen käytäntö salata tiedot turvallisuuden ja yksityisyyden suojaamiseksi. Kuitenkin, kuten Fitbit-laitteiden korjaamattomat haavoittuvuudet ja puutteellinen kommunikaation salaaminen osoittavat, laitteen tunnistetietojen suojaamisessa on puutteita. Nämä puutteet mahdollistavat seurannan ja passiiviset hyökkäykset sillä laitteen tunniste (IDT) lähetetään selkokielisenä. Lisäksi kuka tahansa voi liittää laitteen omaan tiliinsä. FitLock-järjestelmän kehittäjät väittävät kommunikaation olevan salattu jaetun avaimen avulla, mutta he eivät ole onnistuneet salaamaan tunnistetta. FitLock-järjestelmän IDT lähetetään salaamattomana tekstinä molemmissa protokollissa, jolloin käyttäjä on jäljitettävissä. (Zhou & Piramuthu 2014.) Google Glass -laitteissa on havaittu Wi-Fi-kaappauksen riski, vaikka tietyt hyökkäykset, kuten Wi-Fi asennus QR-koodilla, on torjuttu. Langattomien järjestelmien turvallisuuden kannalta on olennaista varmistaa tietojen salaaminen erityisesti lähetettäessä arkaluontoista tietoa, jotta tietoturva ja yksityisyys säilyvät. (Datta & Namin & Chatterjee 2018.) Samsung Gear S3:n GPS- ja Wi-Fi-lokitiedot paljastavat käyttäjän sijaintitietoja. Alkuperäisistä suojauksista huolimatta nämä tiedot ovat tunnistettavissa ja jäljitettävissä. GPS-tallenteet säilyttävät laitteen todellisen sijainnin käyttäjän toimista riippumatta. Wi-Fi-yhteyksiin liittyvistä lokitiedoista voidaan päätellä käyttäjän sijainteja kauppojen ja metroasemien SSID-nimien perusteella. (Park & Riha & Yoon & Lee 2021.)

Älypuhelimet ovat yleisesti siirtyneet käyttämään uusinta BLE-tekniikkaa, kun taas monet puettavat älylaitteet eivät ole päivittyneet vastaamaan viimeisimpiä standardeja. Valmistajat ovat vastuussa ja päättävät turvatoimenpiteiden toteutuksesta. (Barua & Alamin & Hossain & Hossain 2022; Peker & Bello & Perez 2022.) Laitteen pieni koko ja rajallinen kaistanleveys asettavat omat haasteensa tietoturvaratkaisuja suunnitellessa. Pienikokoisina laitteina esimerkiksi älykellot ja aktiivisuusrannekkeet vaativat tehokkaan datan hallinnan ja turvallisuuden tasapainottamista rajoitettujen laskenta- ja

yhteysresurssien kanssa. (Chin & Singh 2016.) Osa turvatoimenpiteistä toteutetaan isäntälohkossa, jossa BLE-laitteet voivat toteuttaa monia turvatoimintoja muun muassa avainten luominen ja salakirjoitus. Mekanismeista osan suoritus on ohjaimessa altistaen ne huonolle toteutukselle. (Barua & Alamin & Hossain & Hossain 2022; Peker & Bello & Perez 2022.) Erityisen huolestuttavaa on Bluetoothin kautta tapahtuva yhteydenmuodostus, joka toteutuu ilman asianmukaista todennusta lisäten merkittävästi tietoturvariskejä (Ioannidou & Sklavos 2021; Peker & Bello & Perez 2022). BLE-tiedonsiirrossa havaitut turvallisuuspuutteet, kuten luvattomien laitteiden pääsy verkkoon, korostavat jatkuvan valvonnan ja päivitysten tarvetta (Chin & Singh 2016; Ioannidou & Sklavos 2021; Peker & Bello & Perez 2022). BLE-tiedonsiirron turvallisuudessa on havaittu merkittäviä haavoittuvuuksia, kaikilla neljällä tutkitulla protokollalla havaittiin turvallisuusongelmia. Ne olivat haavoittuvia tehtyjä hyökkäyksiä, muun muassa imitaatiohyökkäyksiä ja offline-sanakirjahyökkäyksiä, vastaan eikä niissä ollut riittävää suojaa salauksen ja tunnistautumisen varmistamiseksi. (Toorani 2015.)

Ongelmana on, että BLE-standardin mukaiset turvamekanismit eivät aina toimi odotetusti, jolloin laitteet altistuvat seurannalle ja phishing-hyökkäyksille (Peker & Bello & Perez 2022; Silva-Trujillo & González González & Pérez & García Villalba 2023). Älylaitteiden testauksessa havaittiin merkittäviä puutteita pariliitoksen toiminnassa sekä suunnittelun standardoinnin tietoturva-alueella. BLE-standardin mukaiset turvamekanismit eivät toteutuneet. Puutteita havaittiin BLE-tiedonsiirron turvallisuudessa, sillä käyttäjätiedot vaarantuivat lähetettyjen tietojen ollessa salaamattomia ja tietovuoto tapahtui. Osoitteita ei satunnaistettu ja niissä oli kiinteät MAC-osoitteet paljastaen laitteiden tyypin ja version. Joissakin laitteissa ei ole uusinta suojausprotokollaa, vaikka ne toimivat uusimman Bluetooth-version kanssa. (Chin & Singh 2016; Peker & Bello & Perez 2022; Silva-Trujillo & González González & Pérez & García Villalba 2023.) Laitteen tai datan manipulaatio sähkömagneettisen induktion, valon tai ääniaaltojen avulla on merkittävä riski tietoturvalle (Cai & Venkatasubramanian 2018). Kaksi älykelloista ei käytä todennusparia (Silva-Trujillo & González González & Pérez & García Villalba 2023). Haittaohjelmat voivat hyödyntää avoimia Bluetooth-portteja (Cai & Venkatasubramanian 2018). Nämä huomatut puutteet korostavat BLE-laitteiden turvallisuuden merkitystä, erityisesti uhkien kuten passiivisen kuuntelun, laitteiden alhaisien suojauksien vuoksi altistuminen erilaisille hyökkäyksille esimerkiksi brute force ja MAC-osoitteen sormenjäljittelyn estämisessä (Barua & Alamin & Hossain & Hossain 2022; Peker & Bello & Perez 2022).

Turvallisuus on ensiarvoisen tärkeää kahden laitteen viestintäkerrosten välisessä BLE-viestinnässä, heikot paritusprotokollat BLE-laiteiden välillä altistavat laitteet hyökkäyksille. Turvallinen portti on välttämätön tiedon eheyden ja luottamuksellisuuden varmistamiseksi järjestelmän ja käyttäjän välillä. (Barua & Alamin & Hossain & Hossain 2022; Silva-Trujillo & González González & Pérez & García Villalba 2023.) BLE-laitteissa ilmenevät tietovuodot ja etäkoodin suoritukset johtuvat sovelluskerroksen haavoittuvuuksista tiedonkeruussa ja -jakamisessa. Joissakin tapauksissa havaittiin puutteita salauksen ja suojaustason käytössä mobiilisovelluksen ja BLE-laitteen välillä, mikä lisää haavoittuvuutta hyökkäyksille. STM32-dokumentaation mukaan mikroprosessorin pitäisi suojata sisäistä flash-muistia ulkoisilta luku- ja kirjoitusoperaatioilta, mutta tietyissä laitteissa tämä suojaus puuttuu tehden laitteet haavoittuviksi hyökkäyksille, joissa muokataan flash-muistin sisältöä. (Barua & Alamin & Hossain & Hossain 2022.) HCI (Human-Computer Interaction) Snoop Log, on Bluetooth-protokollan osa, joka mahdollistaa tietokoneen ja Bluetooth-laitteen välisen kommunikoinnin. HCI ei estä käyttäjäidentiteetin paljastumista eikä suojaa KCI-hyökkäyksiltä, mikä osoittaa PFS:n (Perfect forward securityn) puutteita ja tarvetta vahvistaa turvallisuusmekanismeja. (Cusack & Antony & Ward & Mody 2017; Toorani 2015.)

Tietoturvahaasteet kasvavat puettavien älylaitteiden käyttömäärän noustessa. Tulokset osoittavat selvästi, että valtuutettujen käyttäjien tunnistaminen ja pääsynhallinta ovat keskeisiä puettavien älylaitteiden tietoturvassa. Vain valtuutetuilla käyttäjillä tulisi olla pääsy laitteisiin, mikä ehkäisee luvattoman käytön ja laitteiden manipuloinnin. (Vaishnavi & Sahana & Guruprasad 2023.) Tämä edellyttää huomiota laitteiden suojaukseen ulkoisia uhkia vastaan. Valmistajien ja kehittäjien tulee ottaa huomioon tietoturvahaasteet ja toteuttaa asianmukaisia turvatoimenpiteitä; vahva salaus, haavoittuvuuksien jatkuva seuranta ja päivitykset sekä käyttäjien tietoturvakoulutus. Näiden toimenpiteiden avulla voidaan varmistaa, että puettavat älylaitteet ovat turvallisia ja että käyttäjien yksityisyys on suojattu niiden käytön aikana. (Vaishnavi & Sahana & Guruprasad 2023.) Laitteiden suunnittelussa on huomioitava jatkuvan yhteyden verkkoon mukanaan tuomat tietovuodon riskit (Datta & Namin & Chatterjee 2018).

IoT-laitteiden suunnittelun valmistajariippuvuus voi lisätä tahattomia tietoturvariskejä (Arias & Wurm & Hoang & Jin 2016). Laitteiden jatkuva teknologinen kehitys on välttämätöntä uusien uhkien torjumiseksi (Datta & Namin & Chatterjee 2018). Kaiken

kerätyn datan laitteessa säilyttäminen luo riskejä, sillä niiden asianmukaisen suojauksen puute altistaa ne väärinkäytölle. Puettavien laitteiden rajoitettu kyky hallita tietokannan tietoja ja käyttäjän rajalliset valtuudet muokata tai poistaa tietoja voivat johtaa yksityisyyden loukkauksiin ja henkilötietojen väärinkäyttöön. Laitteistojen ja ohjelmistojen turvallisuustoimenpiteiden kehittäminen on yhä tärkeämpää, eikä vain ulkoisia uhkia vastaan, vaan myös sisäisiä tietoturvariskejä silmällä pitäen. Ohjelmistopohjaisten suojauksien ohittaminen ja haittakoodin syöttäminen, käynnistysprosessin alttius manipuloinnille ja etäpäivitysten turvallisuuden puutteet lisäävät laitteiden haavoittuvuutta. (Arias & Wurm & Hoang & 2015.) Tietojen paikallinen tallennus ilman salausta ja verkkoturvallisuuden puutteet puettavissa älylaitteissa voivat johtaa merkittäviin tietoturvariskeihin, korostaen jatkuvan valvonnan ja parannettujen suojatoimien tarvetta (Chin & Singh 2016; Vaishnavi & Sahana & Guruprasad 2023).

IoT- ja Big Data -paradigmoissa käyttäjätietojen keräys ja analysointi sekä sijainnin ennustaminen toimintohistorian perusteella tuovat esiin henkilötietojen suojaamisen haasteita älylaitteissa ja IoT-järjestelmissä. Henkilökohtaisten tietojen suojaamattomuus laitteista sovelluksiin siirrettäessä voi aiheuttaa tietovuotoja ja yksityisyyden rikkomuksia. Tämä korostaa tarvetta kehittää sekä ohjelmistojen että laitteistojen turvallisuutta. (Ioannidou & Sklavos 2021.) Valmistajariippuvaisuus ja valvontapalveluiden puute IoT-laitteissa voivat johtaa tahattomiin tietoturvariskeihin ja antaa hyökkääjille mahdollisuuden arkaluonteisen tiedon vuotamiseen tai haittaohjelmien asentamiseen. Avoin lähdekoodi voi tuoda tietoturvaetuja, mutta myös riskejä, joten sen ja suljetun lähdekoodin välistä turvallisuuseroa tulee arvioida huolellisesti. (Arias & Wurm & Hoang & Jin 2015.) Salausratkaisujen virheet ja toimitusketjun haavoittuvuudet, kuten komponenttien väärentäminen tai haittaohjelmien lisääminen laitteisiin, lisäävät turvallisuusriskien kirjoa (Arias & Wurm & Hoang & Jin 2015).

Jatkuvan tietoturvan varmistaminen laitteiden ja ohjelmistojen suunnittelussa ja kehityksessä on elintärkeää, erityisesti ottaen huomioon älylaitteiden ja IoT-järjestelmien kasvava käyttö. Tämä edellyttää keskittymistä myös käyttäjän tunnistautumiseen ja liitettävyyteen liittyviin haasteisiin. Lähes kaikki kunto- ja aktiivisuusseurantalaitteet käyttävät Bluetooth-, ANT-radiota, matkapuhelindataa ja Wi-Fi-verkkoja liitettävyystarkoituksiin. Valtavien tietomäärien luominen tekee tiedonhallinnasta yhden IoT-infrastruktuurien kriittisimmistä haasteista, johon liittyy

liitettävyys-, käsittely-, mediaseuranta- ja tallennustilan hallintaongelmia sekä linkittämisen ongelmia mukaan lukien sijainti- ja henkilökohtaisten tietojen kerääminen. (Ioannidou & Sklavos 2021.)

6.4 Säädökset ja oikeudelliset kysymykset

Voimassa oleva lainsäädäntö, kuten HIPAA, ei kata kaupallisia laitteita eikä niiden keräämiä terveystietoja (Langley 2015). Säädöspuitteita ja tietoturvastrategioita on vahvistettava, jotta edistetään vahvempia turvatoimia ja suojataan käyttäjien yksityisyyttä (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016). Nykyinen standardointi on puutteellinen (Ioannidou & Sklavos 2021). Turvallisuus- ja yksityisyysstandardeja on syytä vahvistaa ja tarkentaa, jotta voidaan suojata käyttäjien yksityisyyttä ja vastata nykyajan teknologian tuomiin haasteisiin (Chin & Singh 2016).

Eurooppalaisen henkilötietodirektiivin vaatimustenmukaisuuden täyttämisen epäonnistuminen on havaittu olevan yksi keskeisimmistä haasteista (Cusack & Antony & Ward & Mody 2017). GDPR:n mukaan henkilötiedot ovat kaikkia tietoja, jotka koskevat tunnistettua tai tunnistettavissa olevaa elävää luonnollista henkilöä. GDPR on laaja lainsäädännöllinen kehys, joka on suunniteltu suojelemaan yksilöiden yksityisyyttä ja henkilötietoja Euroopan unionissa sekä sen ulkopuolella, jos tietoja käsitellään EU:n kansalaisten osalta. GDPR:n vaikutus puettavien laitteiden tietosuojaan ja turvallisuuteen on merkittävä. Asetuksen tavoitteena on luoda tasapainoinen ja yksinkertaistettu sääntely-ympäristö Euroopan unionin yrityksille ja kansalaisille. GDPR:n kehitys etenee teknologisen kehityksen, esimerkiksi IoT:n ja Big Data -paradigmien kanssa, joille tiedonkeruu ja analysointi ovat äärimmäisen tärkeitä. Sen tavoitteena on kattaa kaikki näkökohdat huomioimalla voimakkaasti tekniset termit, kuten Internet-protokollan (IP) osoitteet, sijaintitiedot ja muut ominaisuudet, joita voidaan käyttää yksilön tunnistamiseen. GDPR:n mukaisesti henkilötietojen määrittely on kattavaa ja henkilötietojen suoja on EU:n lainsäädännössä keskeinen prioriteetti. Vaikka monet suositut Android-sovellukset saattavat toimia ilman selkeitä tietosuojakäytäntöjä, GDPR korostaa, että käyttäjien toiminnan kautta kerätyt tiedot ovat muodostumassa todelliseksi valuutaksi, jonka kolmannet osapuolet ostavat. Tämä asetus edellyttää yrityksiä ja organisaatioita, jotka käsittelevät Euroopassa sijaitsevien kansalaisten tietoja, keskittymään henkilön arkaluonteisten tietojen suojeluun. GDPR:n määritelmän mukaan henkilötiedot ovat henkilön arvokasta omaisuutta ja asetus pyrkii

varmistamaan käyttäjien luottamuksen uuteen teknologiaan asettamalla digitaalisen yksityisyyden perusoikeuden etusijalle. (Ioannidou & Sklavos 2021).

Tietosuojalakien vaihtelu globaalisti luo epätasa-arvoa kuluttajien tietosuojassa. Joidenkin maiden tiukat tietosuojalait ja toisten puute aiheuttavat haasteita. Eri maiden väliset erot tietosuojalaeissa korostavat tarvetta maakohtaisten lakien ja säädösten yhtenäistämiselle. (Cusack & Antony & Ward & Mody 2017; Datta & Namin & Chatterjee 2018; Okonkwo & Awolusi & Nnaji 2022.) Erityisesti Yhdysvalloissa puuttuu liittovaltion lainsäädäntö kuluttajien puettaviin älylaitteisiin liittyvien yksityisyysongelmien osalta. Tämä vaatisi yksityisyysstandardeja, joita ei välttämättä ole olemassa nykyisessä lainsäädännössä. (Langley, 2015.) Eri maiden väliset erot IoT-tietoturvan sääntelyssä ja puutteelliset standardit luovat haasteita puettavien älylaitteiden käytölle (Okonkwo & Awolusi & Nnaji 2022).

Maiden väliset erot IoT-tietoturvan säätelyssä, standardien puutteellisuus sekä yhtenäisten säännösten puute kansainvälisellä tasolla antavat mahdollisuuden lakien rikkomiseen, sillä eri alueilla erilaisia tietoja käsitellään erilaisilla lainsäädännöillä. Lakien yhteensovittaminen lisää prosessin monimutkaisuutta. Tämän yhteisen lain puuttuminen IoT-infrastruktuurille voidaan osoittaa aiheutuneen IoT-teknologian nopeasta kehityksestä, kun sääntelyviranomaiset kamppailevat vastaamaan IoT-teknologian oikeudellisiin ongelmiin. On tunnistettu myös tarve globaalille lainsäädännölle WIoT (Wearable Internet of Things) -datan hallinnassa, erityisesti IoT:n turvallisuussäädösten osalta. Yhdysvalloissa ei myöskään ole oikeudellisia säännöksiä tietojen säilytysajasta, mikä luo rikollisuutta edistävän ympäristön palveluntarjoajille. (Okonkwo & Awolusi & Nnaji 2022.)

Yhdysvalloissa HIPAA -lain alaisuudessa toimivat terveystietoja keräävät tahot saavat paljastaa henkilökohtaisen tunnistettavan tiedon ilman yksilön suostumusta, kun se on tarpeen yksilön, yleisen edun tai hoidon ja terveydenhuollon tarkoituksiin. Muita terveystietoja sääteleviä viranomaisia ovat Health Information Technology for Economic and Clinical Health (HITECH), International Organization for Standardization (ISO) ja National Institutes of Standards and Technology (NIST). Näiden viranomaisten rooli ja vaikutus ulottuvat Yhdysvaltojen rajojen ulkopuolelle, vaikka ne alun perin ovatkin Yhdysvaltojen lainsäädännöstä ja organisaatioista lähtöisin. (Okonkwo & Awolusi & Nnaji 2022.)

Valmistajien vastuulla on integroida turvallisuusmekanismeja IoT-laitteiden suunnitteluvaiheessa. Niiden tulisi myös ottaa vastuu tietoturvastrategioiden kehittämisestä, toteuttamisesta ja valvonnasta. Nykyiset nopeat markkinoilletuontiajat ja turvallisuuden sivuuttaminen korostavat tarvetta vahvistaa tietoturvastrategioita sekä kehittää lainsäädäntöä ja standardeja, jotka suojaavat käyttäjien yksityisyyttä. (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023.) Puettavien älylaitteiden käyttöönottoon liittyy olennaisia säädöspuitteita ja oikeudellisia kysymyksiä, joiden kattava tarkastelu on välttämätöntä (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016).

Järjestelmien tulisi täyttää vaatimukset tunnistautumisessa, anonymiteetissä, salauksessa ja liikenteen seurannassa (Okonkwo & Awolusi & Nnaji 2022). Ihmisen fysiologisia tietoja keräävien kuluttajien käyttämien laitteiden osalta on riski, että laitteet eivät noudata turvastandardeja. Tämä asettaa kysymyksiä yksityisyydensuojasta ja oikeudellisesta vastuusta. (Peker & Bello & Perez 2022.) Monilla suosituilla Android-sovelluksilla ei ole tietosuojakäytäntöä. Puettavien laitteiden standardit ovat olemassa ja niiden käyttöä suositellaan muttei vaadita. Vaikka monet puettavat älylaitteet keräävät käyttäjänsä terveystietoja, ne eivät välttämättä ole lääkinnällisiä laitteita, joten niiden ei tarvitse noudattaa tiettyjä turvastandardeja. (Peker & Bello & Perez 2022.) Laitteiden on vaikea saavuttaa sääntelyn vaatimusten mukaisuutta (Cusack & Antony & Ward & Mody 2017; Datta & Namin & Chatterjee 2018). Turvallisuusprotokollan omaavilla laitteilla oli turvallisuusongelmia (Toorani 2015).

Puettavien laitteiden nopea kehitys ja markkinoille tulo korostavat turvatoimien ja yksityisyydensuojan tärkeyttä. Oikeudelliset sääntely-ympäristöt yleensä mukautuvat teknologian kehitykseen noin viiden vuoden kuluttua, eikä nykyiset lait ole valmiita vastaamaan uusien puettavien älylaitteiden teknologioiden myötä nousseisiin uhkiin ja haasteisiin. Kehittäjät pyrkivät luomaan uusia ja tehokkaampia puettavia älylaitteita, mikä lisää kuilua teknologian ja lainsäädännön välillä. (Mills & Watson & Leyland & Kietzmann 2016.) Lait ja standardit määrittävät tietojen keräämistä, mutta osa niistä on osoittautunut tehottomiksi ja ne vanhentuvat nopeasti (Arias & Wurm & Hoang & Jin 2015). Tietoturvastrategioiden ja lainsäädännön on pysyttävä mukana kehityksessä (Mills & Watson & Leyland & Kietzmann 2016).

Ihmisen fysiologisia tietoja keräävien puettavien älylaitteiden ei tarvitse olla sertifioituja eikä noudattaa turvastandardeja, elleivät ne ole luokiteltu lääkinnällisiksi laitteiksi.

Tulevaisuudessa, teknologian kehittyessä tämä luo turvallisuusaukkoja väärinkäytöksiin muun muassa kuntoilun seurantaan käytetyissä puettavissa älylaitteissa. Monia haavoittuvuuksia on ilmennyt viestintäprotokollissa, erityisesti Bluetoothissa. (Silva-Trujillo & González González & Pérez & García Villalba 2023). Jos nämä laitteet eivät ole BLE:n turvallisuussertifioituja, on mahdollista, että vastaavia sertifikaattien poistoja tapahtuu tulevaisuudessa, vaikka kuntoilutietoja kerättäisiin osana lääketieteellisiä tietueita. Tällöin ne rikkovat yksityisyydensuojalakeja (esimerkiksi HIPAA) lääketieteellisissä terveystietueissa. (Peker & Bello & Perez 2022.)

Käyttäjän terveystietoja keräävien puettavien älylaitteiden osalta on havaittavissa lainsäädännöllisiä haasteita. Kun näitä laitteita käytettiin terveydenhuoltoon tai lääketieteellisiin tarkoituksiin, Yhdysvaltain terveysministeriö ja liittovaltion lääkevirasto (FDA) pystyivät asettamaan yksityisyysstandardeja. Niiden toimivalta ja soveltamisala on rajoitettu, sillä puettavia laitteita käytetään nykyään yhä enemmän kuluttajatuotteina. Vuoden 1986 sähköisen viestinnän yksityisyyslaki (ECPA) voisi teoriassa säädellä kuluttajien puettavia älylaitteita, mutta laki on vanhentunut eikä se ota huomioon nykyaikaista viestintätekniikkaa. ECPA:ssa on myös porsaanreikä, joka sallii yritysten luovuttaa asiakastietoja kolmansille osapuolille (Langley 2015). Federal Trade Commission (FTC) onkin havainnut, että mainontatarkoituksiin kerättyjen, käsiteltyjen ja välitettyjen henkilötietojen määrä oli merkittävä (Ioannidou & Sklavos 2021; Langley 2015).

6.5 Käyttäjien rooli ja tietoisuus puettavien älylaitteiden tietoturvassa

Puettavien älylaitteiden integroituminen arkielämään on kasvattanut merkittävästi niiden suosiota. Laitteiden yleistyessä niiden käyttöön liittyvät yksityisyyden ja tietoturvan haasteet ovat nousseet keskiöön, sillä monet käyttäjät ovat osittain tai kokonaan tietämättömiä niiden käyttöön liittyvistä yksityisyyden suojaan ja tietoturvaan liittyvistä riskeistä (Datta & Namin & Chatterjee 2018; Langley 2015) tai heillä on vakavia virheellisiä käsityksiä näihin laitteisiin liittyvistä yksityisyyden riskeistä (Datta & Namin & Chatterjee 2018). Tietämättömyys voi johtaa vakaviin seurauksiin, henkilötietojen vuotamiseen ja tietoturvarikkomuksiin. Laitteiden keräämät arkaluonteiset tiedot, kuten terveys- ja sijaintitiedot, altistavat käyttäjät potentiaalisille tietoturvauhille. Tietojen väärinkäyttö voi johtaa vakaviin seurauksiin käyttäjille. Erityisesti ikääntyvien käyttäjien sekä lasten, tulisi olla tietoisia laitteidensa

tietoturvariskeistä jos laitteet joutuvat vääriin käsiin tai niitä ei valvota asianmukaisesti. (Shukur & Fatlawi 2022.)

Käyttäjien tietämättömyys ulottuu laajasti myös käytäntöihin, joissa henkilötietoja tallennetaan ja myydään eteenpäin. Tämä tapahtuu usein ilman käyttäjän tietoista suostumusta. (Ioannidou & Sklavos 2021; Langley 2015.) Tällainen tietojen käsittely ja jakaminen kohdistetussa markkinoinnissa on yleistä ja herättää huolen siitä, ovatko käyttäjät täysin tietoisia antamiensa tietojen mahdollisista seurauksista (Ioannidou & Sklavos 2021). Kuluttajien puettavien älylaitteiden käyttöönotto heikentää yksityisyyden suojaa, kun sekä henkilötiedot että henkilökohtaiset terveystiedot voidaan kerätä ja jakaa vapaasti (Langley 2015; Shukur & Fatlawi 2022). Myös sijaintia, poliittisia mieltymyksiä, yhteydenpitoa yhteyshenkilöihin, terveydentilaa koskevia hakukyselyjä ynnä muita arkaluonteisia tietoja kerätään ja myydään (Langley 2015). Tärkeää on, että käyttäjät ymmärtävät, miten heidän tietonsa kerätään, käsitellään ja jälleenmyydään eteenpäin ilman heidän täyttä tietoisuuttaan (Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021; Langley 2015). Laajasta vuorovaikutuksesta huolimatta käyttäjät ovat harvoin tietoisia siitä, milloin ja mitä tietoja älylaitteet jakavat internetissä, eivätkä he ole täysin tietoisia siitä, että tämä heidän tietojensa tallentaminen ja jälleenmyynti on yleinen käytäntö. (Ioannidou & Sklavos 2021). Ei ole epäilystäkään siitä, että käyttäjien olisi oltava täysin tietoisia ennen pääsyn myöntämistä laitemoduuleihin, jotka voivat vuotaa arkaluonteisia henkilötietoja, kuten sosiaaliturvatunnuksen. Henkilökohtaisten tietojen keräysprosessi ei tosin ole aina ilmeinen, sillä useimmissa tapauksissa henkilötietojen kerääminen tapahtuu ”hiljaa” käyttäjän jäljelle jääneiden jälkien perusteella hyödyntäen taustamekanismeja, joiden olemassaolo ja toiminnallisuus jätetään usein huomiotta tai käyttäjä ei ymmärrä niitä täysin. Koska älylaitteista ja sosiaalisen verkostoitumisen alustoista on tullut osa jokapäiväistä elämää maailmanlaajuisesti, henkilötietojen jakamisesta on tullut edellytys useimpien digitaalisten sovellusten ja palveluiden käytölle. (Ioannidou & Sklavos 2021.)

IoT mahdollistaa puettavien älylaitteiden yhdistämisen ympärillään oleviin järjestelmiin. Älykellon liittäminen älypuhelimeen tietojen tallentamiseksi ja analysoimiseksi esimerkiksi älykkään kodin hallintaa varten aiheuttaa tietoturvauhkia ja tietovuodon riskejä. (Shukur & Fatlawi 2022.) Myös riski hakkeroinnista kasvaa (Barua & Alamin & Hossain & Hossain 2022). Laitteiden tekniset ominaisuudet, kuten BLE-teknologia ja IoT mahdollistavat laitteiden jäljittämisen ja arkaluonteisten tietojen, kuten terveys- ja

sijaintitietojen, keräämisen. Tämä tuo mukanaan täysin uudentyyppisiä tietoturvariskejä, sillä jos sovelluksella on oikeus käyttää Bluetoothia, se voi yhdistää mihin tahansa BLE-laitteeseen. (Barua & Alamin & Hossain & Hossain 2022.) Ottaen huomioon kulutuslaitteiden valtavan määrän maailmassa, monet julkisesti ostetut BLE-laitteet voidaan helposti jäljittää. Silloin ne käyttäjätiedot, jotka tulisi suojata, ovat helposti hakkerien ja rogue-toimijoiden saatavilla. Markkinoilla olevien BLE-teknologiaa hyödyntävien laitteiden tietosuoja vaihtelee, mutta kuluttajalle harvoin kerrotaan mikä Bluetooth-versio laitteessa on. (Peker & Bello & Perez 2022.) Lisäksi älykotiratkaisujen käyttäjät altistuvat riskeille, kun älykellot ja älypuhelimet vaihtavat tietoja keskenään. Tämä tiedonsiirto voi altistaa käyttäjien tietoja mahdollisille vuodoille tai muille turvallisuusuhille, jos asianmukaisia varotoimia ei ole otettu käyttöön. (Shukur & Fatlawi, 2022; Barua & Alamin & Hossain & Hossain 2022.)

Kun puettavat älylaitteet kehittyvät ja ihmiset muuttavat käyttäytymistään, uusia uhkia ilmaantuu (Mills & Watson & Leyland & Kietzmann 2016). Teknologian kehittyessä ja käyttötapojen muuttuessa olisikin tärkeää, että käyttäjät ovat tietoisia mahdollisista uusista uhista ja ymmärtävät, miten suojata itseään tehokkaasti (Silva-Trujillo & González González & Pérez & García Villalba 2023). Käyttäjien tietoisuutta riskeistä olisi tärkeä lisätä (Ioannidou & Sklavos 2021; Mills & Watson & Leyland & Kietzmann 2016) ja asianmukaisten turvakäytäntöjen noudattamisen merkitystä korostaa (Chin & Singh 2016). Useimmissa tapauksissa kuluttaja tietää laitetta ostaessaan riskit, mutta luottaa liikaa laitteen palveluntarjoajaan (Datta & Namin & Chatterjee 2018). Vastuu laitteiden suojauksesta tulisi olla laitteen tarjoajalla, mutta käytännössä kuluttajan on oltava valveutunut suojaamaan laitteensa oikein. Ongelmana on kuitenkin se, että kaikilla kuluttajilla ei ole tietämystä siitä, kuinka käsitellä ja ylläpitää omaa tietoturvaansa. Ja toisaalta vaikka käyttäjät olisivat tietoisia turvallisuusongelmista, salaustoimenpiteitä ei usein oteta käyttöön eikä päivityksiä tehdä. Tämä johtuu usein joko tiedon puutteesta tai välinpitämättömyydestä luoden haavoittuvuuksia, jotka voivat johtaa henkilötietojen väärinkäyttöön. (Datta & Namin & Chatterjee 2018). Kuluttajien on oltava valveutuneita ja otettava aktiivinen rooli oman tietoturvansa hallinnassa. Käyttäjien tulisi olla täysin tietoisia puettavien älylaitteiden yksityisyys- ja tietoturvaongelmista ennen minkään puettavan laitteen käyttöä. Epäselvät yksityisyys- ja tietoturvaongelmat voivat johtaa epäluottamukseen puettavaa teknologiaa kohtaan. (Shukur & Fatlawi 2022.)

6.6 Laitevalmistajien ja kehittäjien vastuu

IoT-laitteiden suunnitteluprosesseihin liittyy merkittäviä haasteita. Laitteiden kehittäjät eivät aseta turvallisuutta ja yksityisyyttä etusijalle. (Chin & Singh 2016.) Käyttäjien riippuvuus valmistajien suunnitelmista ja sovellusratkaisuista voi altistaa laitteet turvallisuusriskeille. Valmistajien tarjoamat ohjelmistokomponentit sisältävät vianetsintäsymboleita, jotka ovat potentiaalisesti haavoittuvia hyökkäyksille, altistaen laitteet tietovuodoille ja haittaohjelmistojen asennuksille. Tämä voi johtaa tahattomiin rajapintojen paljastumisiin, jotka on suunniteltu ainoastaan vianetsintään tai ohjelmoinnin uudelleenmäärittämiseen. Hyökkääjät voivat hyödyntää näitä rajapintoja laitteen toiminnan hallitsemiseen. Hyökkääjien helppo pääsy laitteisiin korostaa perusteellisen toiminnallisen testauksen ja ohjelmistojen tarkistuksen tärkeyttä ennen tuotantoon päätymistä. Valmistajien vastuulla on integroida tehokkaat turvallisuusmekanismit jo suunnitteluvaiheessa. (Arias & Wurm & Hoang & Jin 2016.) Puettavien älylaitteiden kehittäjien on asetettava turvallisuus ja yksityisyys etusijalle koko laitteen suunnittelu- ja päivitysprosessin ajan, jotta käyttäjätiedot voidaan suojata (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016).

Laitteen kokoonpanovaiheessa flash-muistisiruille ohjelmakuvien kirjoittaminen on kustannustehokkaampaa, kuin valmiiksi ohjelmoitujen komponenttien ostaminen. Laitteiden toiminnallinen testaus ennen tuotantoon päätymistä on välttämätöntä ja edellyttää piirilevyllä olevia ohjelmointiliitäntöjä ja eri komponenttien testauspisteitä. Vaikka näitä liitäntöjä ei useinkaan ole merkitty eivätkä ne ole aktiivisia, niitä ei poisteta testauksen jälkeen. Tämä tarjoaa hyökkääjille reitin koodin injektointiin tai laitteen toiminnan muuttamiseen. Kääntäjien tuottamat binääritiedostot vianetsintäsymboleineen voivat antaa hyökkääjille vihjeitä haavoittuvuuksista. Turvallisuuden varmistamiseksi valmistajien olisi poistettava nämä symbolit ja suljettava testausliitännät ennen tuotteiden lähettämistä markkinoille. (Arias & Wurm & Hoang & Jin 2016.)

Valmistajien kiire tuoda tuotteita markkinoille turvallisuuden kustannuksella korostaa tietoturvastrategioiden, -säännösten ja lainsäädännön tarpeellisuutta (Mills & Watson & Leyland & Kietzmann 2016). Yritysten olisi otettava vastuu puettavan teknologian tietoturvastrategioiden kehittämisestä, toteuttamisesta ja valvonnasta, sillä monet puettavat älylaitteet ovat tällä hetkellä riittämättömästi suojattuja (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016). Puettavien teknologioiden kehittäjien

keskittyessä uusien ja tehokkaampien laitteiden luomiseen, jatkuva tuki vanhemmille versioille ei aina ole taattu. Tämä ja yritysten haluttomuus vanhempien laitteiden säännöllisiin päivityksiin johtavat laajamittaisiin tietoturvaongelmiin. (Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023.) Huomattava osa laitevalmistajista ei tarjoa riittäviä tietoturvakorjauksia, jolloin käyttäjät ovat alttiita hyökkäyksille eikä ohjelmistopäivityksiä tai tietoturvakorjauksia, jotta hyökkäyksen jälkeisiä haittoja voitaisiin lieventää tai estää. Markkinoiden suuren kysynnän vuoksi valmistajat asettavat etusijalle komponenttien optimoinnin kustannusten leikkaamiseksi ja keskittyvät keskeisten toimintojen tarjoamiseen unohtaen kriittiset turvallisuusvaatimukset. (Silva-Trujillo & González González & Pérez & García Villalba 2023.)

Jotkin laitevalmistajat käyttävät epämääräisiä tai epäselviä tietosuojakäytäntöjä, jotta niillä olisi mahdollisimman suuri määräysvalta tai omistusoikeus käyttäjien tietoihin (Datta & Namin & Chatterjee 2018; Langley 2015). Neljän suositun kuntoilussa käytettävän älylaitteen yksityisyyskäytäntöjä analysoitaessa havaittiin, että lähes kaikki palveluntarjoajat väittivät omistavansa käyttäjän terveystiedot ja vain yksi analysoiduista laitteista sallii käyttäjälle mahdollisuuden tietojensa täydelliseen poistamiseen. Yllättäen yksikään näistä organisaatioista ei ilmoittanut käyttäjille yksityisyyskäytäntöjen muutoksista. (Datta & Namin & Chatterjee 2018.) Laitevalmistajilla ja sovelluskehittäjillä on mahdollisuus kerätä käyttäjien terveystietoja ja myydä näitä tietoja ilman käyttäjien suostumusta tai ilmoitusta, mikä nostaa esiin valmistajien vastuun käyttäjien yksityisyyden suojaamisessa. Yksityisyyden suojaa koskevien käytäntöjen ja vaatimusten tulisi olla selkeitä sovellus- ja laitevaatimusten osalta. Käyttäjätietojen myyminen kolmansille osapuolille ja epäilyttävien käyttöoikeuksien myöntäminen tulisi tunnistaa riskiksi. Erilaiset laitteet altistuvat eritasoisille riskeille ja arkaluonteiset tiedot tunnustetaan arvokkaaksi omaisuudeksi nykyisessä IoT-maisemassa, mikä voi johtaa taloudellisiin ja oikeudellisiin seurauksiin. (Chikwetu ym. 2023; Ioannidou & Sklavos 2021; Langley 2015.)

BLE on nykyään yksi yleisimmin käytetyistä teknologioista langattomassa kommunikaatiossa, erityisesti IoT-laitteissa. Sen suosio valmistajien keskuudessa perustuu sen kykyyn mahdollistaa energiatehokas tiedonsiirto laitteiden välillä. Tästä huolimatta juuri tämän laajalti käytetyn teknologian turvallisuus on haaste, joka asettaa suuria vaatimuksia laitevalmistajille ja kehittäjille. Bluetooth SIG (Special Interest Group) ei määrää standardien täydellistä noudattamista, mikä johtaa siihen, että jotkut

valmistajat jättävät huomiotta asianmukaisten turvatoimien toteuttamisen. Vaikka Bluetooth SIG suosittelee tietoturvavaihtoehtojen sisällyttämistä, päätös siitä jää valmistajalle. Turvaominaisuudet ovat osa BLE-standardeja, mutta tutkitut laitteet eivät täysin toteuttaneet BLE:n turvaominaisuuksia. BLE-laitteet pyrkivät olemaan yhteensopivia yhdistäessään, jolloin ne saattavat käyttää alhaisinta saatavilla olevaa Bluetoothin turvaominaisuutta, vaikka edistyneempi ominaisuus olisi saatavilla toiselle paritetuista laitteista. Tämä johtaa tilanteeseen, jossa edistyneemmät turvaominaisuudet jäävät käyttämättä toisessa paritetussa laitteessa. Alhaisen suojauksen BLE-yhteydet altistavat henkilön fysiologiset tiedot, joita voidaan käyttää biometristen autentikointijärjestelmien toistohyökkäyksissä. Järjestelmät luottavat usein puettavien älylaitteiden anturitietoihin sekä yksittäisessä että jatkuvassa tunnistuksessa. Tietojen vuotaessa aiheutuu turvallisuus- ja autentikointihaasteita. Varastettuja fysiologisia tietoja voidaan käyttää väärin etäpalvelujen manipulointiin taloudellisen hyödyn saamiseksi. Suojaamattomat BLE-laitteet ovat alttiita palvelunestohyökkäyksille ja niitä voidaan jopa käyttää hyökkäämään muita laitteita tai langattomia verkkoja vastaan. (Peker & Bello & Perez 2022.)

Avaimettomien lukkojen yleistyessä muun muassa älykotiratkaisuissa ja älypyörissä, niiden suosio perustuu usein BLE-teknologian helppokäyttöisyyteen. Kuitenkin monilta näiden lukkojen valmistajilta puuttuvat riittävät kryptografiset suojatoimet ja turvalliset pariliitokset, mikä vuoksi ne ovat alttiita tietoturvaloukkauksille. (Barua & Alamin & Hossain & Hossain 2022.) Valmistajien on tärkeä huomioida turvallisuusriskit kehittäessään älykoteihin ja muihin sovelluksiin tuotteitaan (Barua & Alamin & Hossain & Hossain 2022; Chin & Singh 2016; Peker & Bello & Perez 2022).

7 Pohdinta

7.1 Tulosten yhteenveto

Puettavien älylaitteiden nopea yleistyminen on herättänyt huolta käyttäjien yksityisyydensuojasta, sillä laitteet altistuvat tietovuodoille ja tietoturvariskeille (Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021; Mills & Watson & Layland & Kietzmann 2016; Shukur & Fatlawi 2022; Vaishnavi & Sahana & Guruprasad 2023). Puettavien älylaitteiden käyttöön liittyvät yksityisyyden ja tietosuojan puutteet on tunnistettu (Shukur & Fatlawi 2022; Ioannidou & Sklavos 2021; Vaishnavi & Sahana &

Guruprasad 2023). Laitteiden jatkuva verkkoyhteys, käyttäjiensä toiminnan jatkuva seuraaminen internetissä sekä kyky kerätä arkaluontoisia tietoja korostavat tehokkaan tietosuojan ja yksityisyyden hallinnan tarvetta, myös työpaikkojen verkoissa (Chikwetu ym. 2023; Ioannidou & Sklavos 2021; Mills & Watson & Layland & Kietzmann 2016; Shukur & Fatlawi 2022; Vaishnavi & Sahana & Guruprasad 2023). Puettavien laitteiden integrointi laajempiin IoT-verkkoihin kasvattaa verkkojen kautta tapahtuvien hyökkäysten mahdollisuuksia, vaarantaen tietojen eheyden ja luottamuksellisuuden (Shukur & Fatlawi 2022; Barua & Alamin & Hossain & Hossain 2022; Vaishnavi & Sahana & Guruprasad 2023).

Älysovellukset pyytävät laajoja käyttöoikeuksia herättäen huolta tietosuojan epäjohdonmukaisuuksista. Puettavat laitteet, kuten kameralla varustetut älylaitteet, voivat tallentaa ja jakaa arkaluonteisia tietoja ilman käyttäjän suostumusta. (Chin & Singh 2016; Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021; Shukur & Fatlawi 2022.) Tiedot myös tallennetaan paikallisesti ilman salausta (Chin & Singh 2016). Puettavat älylaitteet ovat yhä henkilökohtaisempia yhdistyessään käyttäjän muihin tietojärjestelmiin, kuten älypuhelimiin ja tietokoneisiin, jotka toimivat portteina laajempiin laitteistossa säilytettyihin tietoihin (Mills & Watson & Leyland & Kietzmann 2016). Kuntoseurantasovellukset hyödyntävät laitetietoja käyttäjän tietojen optimointiin (Ioannidou & Sklavos 2021), mutta seuranta voi tapahtua ilman käyttäjän tietoisuutta (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Zhou & Piramuthu 2014). Arkaluonteiset tiedot on suojattava, jotta käyttäjän elämäntavat eivät paljastu (Ioannidou & Sklavos 2021). Fysiologisia mittauksia yhdistelemällä voidaan päätellä käyttäjän tietoja (Datta & Namin & Chatterjee 2018), ja jopa älypuhelimen anturit voivat tunnistaa käyttäjän (Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021).

Sensoridataa jaettaessa uudelleentunnistamisen riski voidaan minimoida muttei täysin eliminoida. Pelkkä tunnistetietojen pidättäminen ja julkisista tietovarastoista poistaminen ei ole riittävää yksityisyyden turvaamiseksi. (Chikwetu ym. 2023.) Laitteiden hallinta voidaan menettää, jolloin syntyy riski arkaluontoisten tietojen vuotamiselle, vaarantumiselle, anastamiselle, tuhoamiselle tai muuttamiselle. Merkittävä riski on myös vahvojen salasanojen puute. Käyttäjää voidaan johtaa harhaan virheellisillä tiedoilla tai hänen fyysistä turvallisuuttansa vaarantaa laitteita vahingoittamalla tai hakkereiden häiritessä niiden toimintaa. (Cai & Venkatasubramanian 2018; Mills & Watson & Leyland & Kietzmann 2016; Vaishnavi & Sahana & Guruprasad 2023.) Osa haittaohjelmista jää huomaamatta normaaleissa

testausmenetelmissä, niiden havaitseminen vaatii kalliita erikoistestejä (Arias & Wurm & Hoang & Jin 2016; Mills & Watson & Leyland & Kietzmann 2016).

Tietoturvahaasteet kasvavat puettavien älylaitteiden käyttömäärän noustessa. Valmistajien vastuulla on kehittää ja toteuttaa tehokkaat tietoturvastrategiat. (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023.) Laitteiden suunnittelussa on huomioitava jatkuvan yhteyden verkkoon mukanaan tuomat tietovuodon riskit (Datta & Namin & Chatterjee 2018). Valmistajien ja kehittäjien on toteuttava asianmukaiset turvatoimenpiteet; vahva salaus, haavoittuvuuksien jatkuva seuranta, päivitykset sekä käyttäjien tietoturvakoulutus. Näiden toimenpiteiden avulla voidaan varmistaa, että puettavat älylaitteet ovat turvallisia ja käyttäjien yksityisyys on suojattu niiden käytön aikana. (Vaishnavi & Sahana & Guruprasad 2023.) Valitettavasti laitevalmistajat eivät usein aseta turvallisuutta etusijalle suunnittelussa. Kehittäjien tulisi keskittyä turvallisuuteen ja yksityisyyteen laitteen koko elinkaaren ajan. (Arias & Wurm & Hoang & Jin 2016; Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023.) Laitteiden turvallisuusongelmat johtuvat osittain valmistajien haluttomuudesta tehdä säännöllisiä päivityksiä vanhempiin laitteisiin ja tukea vanhempia laiteversioita, mikä avaa ovet laajamittaisille tietoturvaongelmille (Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023). Valmistajariippuvaisuus ja valvontapalveluiden puute IoT-laitteissa johtaa tahattomiin tietoturvariskeihin ja antaa hyökkääjille mahdollisuuden arkaluonteisen tiedon vuotamiseen tai haittaohjelmien asentamiseen (Arias & Wurm & Hoang & Jin 2015).

Tämän opinnäytetyön tulokset osoittavat selvästi, että valtuutettujen käyttäjien tunnistaminen ja pääsynhallinta ovat keskeisiä puettavien älylaitteiden tietoturvassa. Vain valtuutetuilla tulisi olla pääsy laitteisiin, jolloin ehkäistään luvaton käyttö ja laitteiden manipulointi. (Vaishnavi & Sahana & Guruprasad 2023.) Tuloksista kävi ilmi, että laitteiden suunnitteluvaiheessa tapahtuvat valinnat, kuten avoimen ja suljetun lähdekoodin ohjelmistojen sekä laitteiston suunnittelun valinnat, vaikuttavat laitteen alttiuteen hyökkäyksille (Ioannidou & Sklavos 2021; Peker & Bello & Perez 2022).

Laitteen pieni koko ja rajallinen kaistanleveys asettavat omat haasteensa tietoturvaratkaisuja suunnitellessa (Chin & Singh 2016). Ohjelmistohaavoittuvuudet johtuvat paitsi matemaattisista haasteista, myös toteutusvirheistä. Vahvojen

salasanojen puute ja kriittiset haavoittuvuudet kryptografisissa järjestelmissä mahdollistavat laitteisiin kohdistuvat etähyökkäykset ja sallivat väärennetyn ohjelmiston asennuksen. (Arias & Wurm & Hoang & Jin 2016; Mills & Watson & Pitt & Kietzmann 2016.) Järjestelmien tulisi täyttää vaatimukset tunnistautumisessa, anonymiteetissä, salauksessa ja liikenteen seurannassa (Okonkwo & Awolusi & Nnaji 2022). Laitteen tunnistetietojen suojaamisessa on puutteita. Nämä puutteet mahdollistavat seurannan ja passiiviset hyökkäykset. (Zhou & Piramuthu 2014.) Alkuperäisistä suojauksista huolimatta tiedot ovat tunnistettavissa ja jäljitettävissä. GPS-tallenteet säilyttävät laitteen todellisen sijainnin käyttäjän toimista riippumatta. Wi-Fi-yhteyksiin liittyvistä lokitiedoista voidaan päätellä käyttäjän sijainteja kauppojen ja metroasemien SSID-nimien perusteella. (Park & Riha & Yoon & Lee 2021.)

Teknologiset ratkaisut ja menetelmät ovat avainasemassa puettavien laitteiden turvallisuuden parantamisessa (Arias & Wurm & Hoang & Jin 2015). Tutkimukset osoittavat, että laitteet ovat alttiita heikoille todennusmekanismeille, salaamattomille yhteyksille ja seurannalle mahdollistaen luvattoman pääsyn ja tietovuodot (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Mills & Watson & Leyland & Kietzmann 2016; Peker & Bello & Perez 2022). Valmistajien ja kehittäjien on omaksuttava uusia, korkeampia turvallisuusstandardeja vastatakseen näihin haasteisiin (Barua & Alamin & Hossain & Hossain 2022; Shukur & Fatlawi 2022; Toorani 2015). Erityisesti BLE-teknologian yleistyminen on tuonut uusia turvallisuushaasteita, kuten haavoittuvuuksia yhteydenmuodostuksessa ja tiedonsiirrossa (Arias & Wurm & Hoang & Jin 2015; Chin & Singh 2016; Ioannidou & Sklavos 2021; Peker & Bello & Perez 2022). Näihin haasteisiin vastaaminen edellyttää jatkuvaa valvontaa ja päivityksiä (Chin & Singh 2016; Ioannidou & Sklavos 2021; Peker & Bello & Perez 2022). Joissakin laitteissa ei ole uusinta suojausprotokollaa, vaikka ne toimivat uusimman Bluetooth-version kanssa. Lisäksi puutteet turvallisuudessa, kuten salaamattomat tiedonsiirrot ja kiinteät MAC-osoitteet, altistavat laitteet tietovuodoille ja hyökkäyksille. (Chin & Singh 2016; Peker & Bello & Perez 2022; Toorani 2015; Silva-Trujillo & González González & Pérez & García Villalba 2023.) Haittaohjelmat voivat hyödyntää avoimia Bluetooth-portteja (Cai & Venkatasubramanian 2018).

BLE-teknologiaa hyödyntävät laitteet Google Glass, Fitbit ja Samsung Smartwatch osoittautuivat alttiiksi monenlaisille hyökkäyksille, kuten Wi-Fi-kaappauksille ja QR-koodihyökkäyksille, joiden seurauksena käyttäjien hallinta laitteistaan ja tietojen turvallisuus vaarantuivat. Heikko todentaminen, salauksen puute ja suojaamaton

verkko altistivat laitteet erilaisille hyökkäyksille ja käyttäjän sijainnin jäljittämiselle. (Chin & Singh 2016; Peker & Bello & Perez 2022.) Turvallisuusanalyysit paljastivat, että monet laitteet, kuten Nest Thermostaatit, ovat alttiita debug-rajapintojen ja heikkojen kryptografisten toteutusten kautta tapahtuville manipulaatioille ja luvattomalle pääsylle (Arias & Wurm & Hoang & Jin 2016). BLE-protokollan tiedonsiirron turvallisuudessa havaittiin merkittäviä haavoittuvuuksia, ja kaikilla neljällä tutkitulla protokollalla havaittiin turvallisuusongelmia (Toorani 2015). Ohjelmakuvien eheys ja aitous etäpäivityksissä on kriittistä (Arias & Wurm & Hoang & Jin 2016). Langattomien järjestelmien, kuten BLE:n, turvallisuuspuutteet altistavat laitteet seurannalle ja phishing-hyökkäyksille. BLE-tiedonsiirrossa on havaittu puutteita sekä turvallisuudessa että pariliitosmekanismeissa. (Barua & Alamin & Hossain & Hossain 2022; Peker & Bello & Perez 2022.)

Teknologian kehittyessä nykyiset lait ja standardit, kuten HIPAA Yhdysvalloissa, eivät ole pysyneet ajan tasalla kaupallisten laitteiden keräämien terveystietojen tietoturvan osalta. Tarve kehittää ja ylläpitää ajantasaista lainsäädäntöä ja standardeja sekä vahvistaa tietosuojakäytäntöjä korostuu IoT-laitteiden ja niiden integroitumisen myötä. (Chin & Singh 2016; Langley 2015; Mills & Watson & Leyland & Kietzmann 2016; Vaishnavi & Sahana & Guruprasad 2023.) Tietosuojalakien vaihtelu maittain luo epätasa-arvoa kuluttajien tietosuojassa ja puuttuvat standardit luovat haasteita (Cusack & Antony & Ward & Mody 2017; Datta & Namin & Chatterjee 2018; Okonkwo & Awolusi & Nnaji 2022). Käytössä olevat standardit olivat testauksessa haavoittuvaisia useille hyökkäyksille (Toorani 2015).

GDPR:n vaatimustenmukaisuuden täyttämisen epäonnistuminen on havaittu olevan yksi keskeinen haaste. Erityisesti käyttäjätietojen omistajuus ja käsittely ovat epäselviä ja monet Android-sovellukset toimivat ilman selkeitä tietosuojakäytäntöjä puutteellisen standardoinnin vuoksi. Tämä johtaa siihen, että käyttäjien toiminnan kautta kerätyt tiedot muuttuvat kaupallisesti arvokkaaksi valuutaksi. (Cusack & Antony & Ward & Mody 2017; Ioannidou & Sklavos 2021.)

Käyttäjien tietoisuus yksityisyyden riskeistä on matala ja väärät käsitykset ovat yleisiä siitä, miten tietoja käytetään tai myydään. Tietosuojan näkökulmasta erityisen ongelmallista on, että käyttäjätietojen omistajuus on usein epäselvä. Laitteet sekä tallentavat että jakavat tietoja joita käytetään laajasti mainonnassa ja markkinointistrategioissa ilman käyttäjien suostumusta. Kuluttajien tulisi olla aktiivisia ja

valveutuneita tietoturvansa hallinnassa ja ymmärtää myös heidän oman toimintansa tärkeys, esimerkiksi päivitysten ja salaustoimenpiteiden tekemisen suhteen. (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021; Langley 2015; Mills & Watson & Leyland & Kietzmann 2016; Shukur & Fatlawi 2022; Zhou & Piramuthu 2014.)

7.2 Eettisyys ja luotettavuus

Opinnäytetyön jokaisen vaiheen tekemisessä noudatettiin hyviä tieteellisiä käytäntöjä eli ollaan rehellisiä, toteutetaan yleistä huolellisuutta ja tarkkuutta tutkimustyössä, tutkimusten ja niiden tulosten arvioinnissa sekä tulosten tallentamisessa ja esittämisessä (TENK 2023). Opinnäytetyötä varten ei tarvittu eettistä ennakkoarviointia eikä tutkimuslupaa koska kyseessä on tutkijalähtöinen kirjallisuuskatsaus.

Tässä opinnäytetyössä käytössä oli tieteellisen tutkimuksen kriteerien mukaiset ja eettisesti kestävät tiedonhankinta-, tutkimus- ja arviointimenetelmät, ja opinnäytetyö toteutettiin tieteellisen tiedon luonteeseen kuuluvalla avoimuudella ja vastuullisella tiedeviestinnällä tuloksia julkaistaessa. Opinnäytetyössä otetaan muiden tutkijoiden saavutukset ja työ asianmukaisella ja kunnioittavalla tavalla huomioon viittaamalla asianmukaisesti heidän julkaisuihinsa antaen arvo ja merkitys joka heidän saavutuksiinsa kuuluu. Opinnäytetyö suunniteltiin, toteutettiin ja raportoitiin sekä siinä syntyneet tietoaineistot tallennettiin tieteelliselle tiedolle asetettujen vaatimusten edellyttämällä tavalla. (TENK 2023.) Opinnäytetyö käytettiin jokaisessa työvaiheessa Turnitin-palvelussa plagioinnin välttämiseksi. Turnitin on järjestelmä, joka vertaa palautetun tiedoston tekstiä verkosta löytyviin alkuperäisiin aineistoihin ja kuvaa yhtäläisyydet prosentteina.

Scoping katsaus on luotettava tapa kartoittaa laajasti olemassa olevaa tietoa varsinkin ajankohtaisesta aiheesta. Tämän menetelmän valinta puettavien älylaitteiden tietoturvariskien kartoittamiseksi oli perusteltu, sillä se mahdollistaa kattavan ja ajantasaisen tiedon keräämisen, mukaan lukien manuaalisen tiedonhaun. Katsauksen luotettavuuden takaamiseksi valintaprosessi suunniteltiin ja toteutettiin huolellisesti, vertaisarvioitujen artikkeleiden seulonta toimi ensisijaisena rajauksena tietokantahauissa, joilla pyrittiin tietoisesti varmistamaan laadukas aineisto. Katsaukseen valittiin vain vertaisarvioituja artikkeleita ja vertaisarviointi oli jo haun rajauksena tietokantahauissa, silti työn edetessä tietokannoista poistui yhteensä kuusi

artikkelia, osa vertaisarvioinneissa ilmenneiden epäselvyyksien vuoksi, osan syytä ei mainittu. Artikkelien poistumisen myötä aineistohakuun otettiin vielä yksi tietokanta lisää, jottei aineiston pääpaino olisi manuaalihaun tuloksissa ja kirjallisuuskatsauksen luotettavuus kärsisi. Tässä tapauksessa scoping katsaus menetelmänä antoi tähän mahdollisuuden, jotta saatiin kattava kuva aiheesta.

Artikkelien poistuminen tietokannoista valinnan ja aineiston tarkemman läpikäynnin aikana toi esille jatkuvan laadunarvioinnin merkityksen, joka toteutettiin tässä opinnäytetyössä JBI-kriteeristön avulla. Laadunarvioinnin avulla varmistettiin artikkeleiden soveltuvuus ja vahvistettiin tulosten validiutta. Käytettyjen tietokantojen laatu ja JBI-kriteeristön mukainen aineistojen laadunarviointi auttoivat varmistamaan, että katsaukseen valittujen artikkeleiden laatu täytti asetetut vaatimukset. Laadunarvioinnin merkitys korostui entisestään artikkelien poistumisen myötä vahvistaen tarpeen huolelliseen laadunvalvontaan, jotta katsaukseen valittujen artikkeleiden laatu voitiin varmistaa parhaalla mahdollisella tavalla.

Aineiston analysointi on katsauksen tekemisen keskeinen osa, joka suoritettiin huolellisesti ja yksityiskohtaisesti yhden tekijän toimesta. Tässä prosessissa keskityttiin tunnistamaan ja dokumentoimaan kaikki olennaiset tiedot ja teemat huolella. Työssä varmistettiin, että sanavalinnat olivat harkittuja ja hyvin suomennettuja. Kaikki keskeiset teemat käsiteltiin kattavasti, mikä takasi katsauksen perusteellisuuden.

Teemoittelu analyysimenetelmänä sopi tähän opinnäytetyöhön hyvin tarjoten rakenteen ja selkeyden käsiteltävälle tietomäärälle. Teemoittelu suoritettiin kahdesti uudelleen poistettujen artikkeleiden vuoksi, mikä osaltaan auttoi varmistamaan, että jokainen teema vastasi tutkimuksen tämänhetkistä tilaa. Moni aihealue sijoittui useamman teeman alle johtuen niiden moniulotteisuudesta ja eri näkökulmista, jotka esiintyivät tutkimusaineistossa. Tämä toi tuloksiin tiettyä toiston tunnetta, vaikka sama aihe linkittyi aina hieman erilaiseen kontekstiin tai tarkasteltiin teeman mukaan eri suunnasta. Jatkossa tämän aiheen katsauksen tekemistä voisi mahdollisesti tehostaa hyödyntämällä aikaisemmissa tutkimuksissa käytettyjä valmiita teemoja. Tällöin tulokset olisivat helpommin jaoteltavissa ja esimerkiksi BLE käsiteltäisiin yhden teeman alla, mikä helpottaisi lukijaa ymmärtämään kokonaisuuden. BLE:n on todettu olevan iso osa puettavien älylaitteiden tietoturvaongelmista ja se on iso kokonaisuus, jonka sisällyttäminen tähän työhön oli haaste. Toisaalta sen poisjättäminen puettavien älylaitteiden tietoturvariskeistä olisi antanut aiheesta suppean kuvan.

Saadut tulokset ovat merkittäviä ja korostavat tietoturvaongelmien monimuotoisuutta lisäten ymmärrystä tietoturvariskeistä ja korostaen standardien sekä lainsäädännön päivitysten tarvetta. Työ tarjoaa arvokasta tietoa terveydenhuollon toimijoille, laitevalmistajille ja tutkijoille, jotka kehittävät ja käyttävät digitaalista terveydenhuoltoa.

7.3 Tulosten tarkastelua ja johtopäätöksiä

Tässä opinnäytetyössä pyrittiin löytämään vastaus kirjallisuuskatsauksen avulla tutkimuskysymykseen -Mitkä ovat yleisimmät puettaviin älylaitteisiin liittyvät tietoturvariskit? Katsauksen tulokset ovat yleisesti ottaen linjassa aiempien tutkimuksien tulosten kanssa. Opinnäytetyön tulokset osoittavat, että puettavien älylaitteiden käytön mukanaan tuomat tietosuojan ja yksityisyyden haasteet ovat erittäin moninaiset ja laajat, ulottuen yksityisyyden loukkauksista ja laitteiden teknisen turvallisuuden haasteista aina suoriin fyysisiin turvallisuusuhkiin. Laitteiden kyky kerätä jatkuvasti dataa käyttäjän toiminnasta on jo pitkään ollut huolestuttavaa. Erityisesti otettaessa huomioon laitteiden yhdistyminen laajempiin IoT-verkkoihin, jolloin riski käyttäjän henkilökohtaisiin yksityistietoihin pääsyyn kasvaa. (Weber 2015: 619.) Samaan päädytään tässä katsauksessa, puettavien laitteiden integrointi laajempiin IoT-verkkoihin kasvattaa verkkojen kautta tapahtuvien hyökkäysten mahdollisuuksia, vaarantaen tietojen eheyden ja luottamuksellisuuden (Shukur & Fatlawi 2022; Barua & Alamin & Hossain & Hossain 2022; Vaishnavi & Sahana & Guruprasad 2023).

Teknologian nopea kehitys ei ainoastaan muuta nykyisiä haasteita, vaan luo myös uusia uhkia, joiden tunnistaminen vaatii jatkuvaa huomiota ja sopeutumista (Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021). Tämä vastaa aikaisemmissa tutkimuksissa esitettyjä huolenaiheita, joiden mukaan tietoturvariskien tunnistaminen ja hallinta on entistä monimutkaisempaa teknologian nopean kehityksen myötä (Watts 2016; Weber 2015). Tietoturvahaasteiden todettiin myös lisääntyvän puettavien älylaitteiden käyttömäärien noustessa (Chin & Singh 2016; Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021; Mills & Watson & Leyland & Kietzmann 2016; Shukur & Fatlawi 2022; Silva-Trujillo & González González & Pérez & García Villalba 2023; Vaishnavi & Sahana & Guruprasad 2023).

Laitteiden kyky jatkuvasti seurata käyttäjiä ja kerätä arkaluonteisia tietoja, kulutustottumuksia ja jopa sijaintitietoja ilman selkeää suostumusta on herättänyt huolta, samoin kuin älysovellusten pyytämät laajat käyttöoikeudet ja sensoridatan

käsittely. Käyttäjät eivät ole tietoisia siitä, miten tietoja käytetään tai myydään kaupallisiin tarkoituksiin sillä laitteet sekä tallentavat että jakavat tietoja käyttäen niitä laajasti mainonnassa ja markkinointistrategioissa ilman suostumusta. (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Datta & Namin & Chatterjee 2018; Ioannidou & Sklavos 2021; Langley 2015; Mills & Watson & Leyland & Kietzmann 2016; Shukur & Fatlawi 2022; Zhou & Piramuthu 2014.) Myös aiemmin on oltu huolestuneita aiheesta, sillä kolmansille osapuolille, esimerkiksi kaupoille, voidaan myydä henkilöstä koostettu informaatio (Watts 2016: 58). Tiedossa myös oli, että IoT-laitteet yhdistävät monesta eri kohteesta keräämänsä tiedot massadatan avulla muodostaen henkilöstä profiilin tyyppisen tiedoston (Watts 2016: 58; Weber 2015: 619). Tässä katsauksessa tuloksista ilmeni, että sensoridataa jaettaessa uudelleentunnistamisen riski voidaan minimoida muttei täysin eliminoida (Chikwetu ym. 2023). Vaikka GDPR ja muut yksityisyydensuojaa koskevat lainsäädännöt tarjoavat teoreettisen viitekehyksen henkilötietojen suojeluun, on aiemmissa tutkimuksissa huomattu käytännön toteutuksen erityisesti puettavien laitteiden kohdalla osoittautuneen puutteelliseksi (Watts 2016; Weber 2015; Folk & Hurley & Kaplow & Payne 2015: 4). Tämä asettaa GDPR:n vaatimustenmukaisuuden kyseenalaiseksi ja korostaa, että haasteet eivät rajoitu ainoastaan tietosuojaan, vaan myös tietoturvan tekniseen toteutukseen, missä puettavien laitteiden suunnittelu ja valmistus eivät aina täytä tietoturvan vaatimuksia (Cusack & Antony & Ward & Mody 2017; Ioannidou & Sklavos 2021). Aiemman tutkimuksen mukaan se, että laki kieltää tunnistettavien henkilötietojen keräämisen, on kierrettävissä IoT:ssä sillä perusteella, että tiedot eivät liity suoraan tiettyyn henkilöön, vaikka ne olisivatkin henkilökohtaisia (Ahlmeyer & Chircu 2016: 22–23).

Aiemmissa tutkimuksissa on todettu, ettei puettavien älylaitteiden tietoturvan sääntely pysy kehityksen tahdissa (Folk & Hurley & Kaplow & Payne 2015: 4), mikä nähdään tässä kirjallisuuskatsauksessa esiintyvien tulosten valossa myös nykyhetkellä ajankohtaisena. Älylaitteet yhä useammin keräävät ja prosessoivat herkkiä henkilötietoja, joiden väärinkäyttö kolmansien osapuolien toimesta on kasvava huoli. Tämän vuoksi laitteiden suunnittelu ja ohjelmistojen kehittäminen vaativat entistä syvempää ymmärrystä tietoturvasta ja korostaa laitekehittäjien, -suunnittelijoiden ja -toimittajien vastuuta. Laitteiden suunnittelussa tulisi ottaa huomioon paitsi uudet tietoturvariskit, myös käyttäjän tietoisuus ja valmiudet reagoida tietoturvauhkiin. (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016). Käyttäjien tietoisuuden merkitys heidän oman datansa hallinnassa ja suojaamisessa onkin noussut esille paitsi

tämän opinnäytetyön tuloksissa (Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad 2023) myös aikaisemmissa tutkimuksissa, joissa todettiin sekä IoT-laitteen käyttäjän että tarjoajan saattavan olla tietämättömiä siitä, että laitteesta puuttuu tietoturvasuojaus (Folk & Hurley & Kaplow & Payne 2015: 4). Tutkimusten tulokset korostavat, että valmistajien toimet laitteiden tietoturvan ja yksityisyydensuojan varmistamisessa ovat keskeisiä, mutta käyttäjien tietoisuuden lisääminen oman datan käytöstä ja suojauksesta on yhtä lailla olennaista. Käyttäjien on yhä tärkeämpää ymmärtää, miten heidän tietojaan kerätään, käsitellään ja jaetaan. Heidän tulisi oppia, kuinka hallita omaa tietosuojaansa ja välttää potentiaalisia uhkia. Käyttäjillä tulisi olla oikeus omistaa omat tietonsa. Tämä on erityisen merkittävää, kun otetaan huomioon laitteiden välisen kommunikaation näkymättömyys ja käyttäjien tietämättömyys tietoturvapuutteista. (Folk & Hurley & Kaplow & Payne 2015: 4; Ioannidou & Sklavos 2021; Vaishnavi & Sahana & Guruprasad 2023.)

Tuloksissa oltiin yhtämielisiä siitä, että on valmistajien vastuulla kehittää ja toteuttaa tehokkaat tietoturvastrategiat (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023). Aiemmin tunnistettu yksityisyydensuojan takaamisen ongelma, laitteiston päivitysten ajantasalla pysymättömyys (Folk & Hurley & Kaplow & Payne 2015: 4), toistui myös tämän katsauksen tuloksissa (Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023).

Teknologian nopea edistyminen ja uusien laitteiden jatkuva tulva markkinoille tuovat esiin aiemmin tuntemattomia tietoturvariskejä. Esimerkiksi BLE-teknologian suosion kasvu on herättänyt kysymyksiä sen turvallisuudesta ja luotettavuudesta tiedonsiirrossa. Jo aiemmissa tutkimuksissa on todettu BLE-tekniikan laajan käyttöönoton johtaneen uudentyyppisiin tietoturvariskeihin, jotka vaatisivat toimivia salausprotokollia ja todentamisprosesseja. (Seneviratne ym. 2017.) Laitteiden valmistajien tulisi kehittää kattavampia suojausstrategioita, jotka vastaavat standardeja nykyisissä sekä myös tulevissa teknologisissa innovaatioissa (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023). Tämän opinnäytetyön tulokset korostavat tarvetta keskittyä käyttäjien tietoisuuden lisäämiseen (Shukur & Fatlawi 2022), selkeämpien käyttäjän omistajuutta koskevien sääntöjen luomiseen (Chin & Singh 2016; Cusack & Antony & Ward & Mody 2017; Ioannidou & Sklavos 2021; Mills & Watson & Leyland & Kietzmann 2016; Zhou & Piramuthu 2014) ja palveluntarjoajien vastuun korostamiseen

tietoturvapäivitysten osalta (Chin & Singh 2016; Mills & Watson & Leyland & Kietzmann 2016; Silva-Trujillo & González González & Pérez & García Villalba 2023), jotta voidaan varmistaa käyttäjän yksityisyyden suoja.

7.4 Jatkotutkimusehdotuksia

Aihetta on tutkittu viime aikoina paljon johtuen alan nopeasta kehityksestä ja laitteiden käytön räjähdysmäisestä kasvusta. Puutteet lainsäädännässä ja standardeissa on tunnistettu ja niitä ollaan korjaamassa EU:n uuden radiolaitedirektiivin myötä. Jatkossa tämän direktiivin vaikutusta puettavien älylaitteiden tietoturvaan ja -suojaan on syytä tarkastella siirtymäajan päätyttyä. Selvitys standardoinnin ja turvasertifikaattien merkityksestä BLE-laitteiden turvallisuudelle olisi myös tärkeää laitteiden ja yhteyksien kehittyessä. Tietoturvakoulutus käyttäjille mainittiin useammassakin tutkimuksessa, joten tutkimus siitä, kuinka tietoturvakoulutus vaikuttaa käyttäjien käyttäytymiseen ja laitteiden turvallisuuteen olisi tarpeellista tehdä. Myös kuluttajien rooli ja vastuu muun muassa päivitysten teosta nousi yhdeksi tietoturvariskeistä tutkimuksissa. Jatkossa olisi hyvä selvittää, miten kuluttajien tietoisuus ja valitsemat turvallisuuskäytännöt vaikuttavat laitteiden turvallisuuteen ja yksityisyyden suojaan.

Lähteet

Abbott 2017. Continuous Glucose Monitoring. <https://freestylediabetes.co.uk/managing-and-monitoring/continuous-glucose-monitoring>. Viitattu 3.5.2023.

von Alfthan, Katja & Hyry, Jaakko 2020. Hyvinvointi-Mittaaminen –Kansalaiskysely Suomi, Saksa, Ranska ja Hollanti total 2020-raportti. Sitra. <https://www.sitra.fi/app/uploads/2020/10/hyvinvointi-mittaaminen-kansalaiskysely-suomi-saksa-ranska-ja-hollanti.pdf>. Viitattu 10.5.2023.

Ahlmeyer, Matthew & Chircu, Alina M. 2016. Securing the Internet of Things: A review. Issues in information Systems 17 (4). p. 21–28.

Arias, Orlando & Wurm, Jacob & Hoang, Khoa & Jin, Yier 2015. Privacy and Security in Internet of Things and Wearable Devices. IEEE Transactions on Multi-Scale Computing Systems, 2015 Vol. 1 (2).

Arksey, Hilary & O'Malley, Lisa 2005. Scoping studies: Towards a methodological framework. International journal of social research methodology 2005, Vol.8 (1), p.19-32.

Atzori, Luigi & Lera, Antonio & Morabito Giocomo 2010. The Internet of Things: A survey. Computer Networks Vol. 54 (15). p. 2787–2805.

Barua, Arup & Alamin, Abdullah Al. & Hossain, Shohrab & Hossain, Ekram 2022. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. IEEE Open Journal of the Communications Society 2022: Volume: 3. Publisher: IEEE.

Bluetooth.com 2015. <http://www.bluetooth.com/Pages/Bluetooth-Smart.aspx>. Viitattu 12.5.2023.

Cai, Hang & Venkatasubramanian, Krishna K 2018. Detecting data manipulation attacks on physiological sensor measurements in wearable medical systems. EURASIP Journal on Information Security Vol. 2018, Article number: 13 (2018). DOI: 10.1186/s13635-018-0082-y.

Chikwetu, Lucy & Miao, Yu & Woldetensae, Melat K. & Bell, Diarra & Goldenholz, Daniel M. & Dunn, Jessilyn 2023. Does deidentification of data from wearable devices give us a false sense of security? A systematic review. Lancet Digit Health 2023 Apr;5(4): p. 239–247. DOI: 10.1016/S2589-7500(22)00234-5.

Chin, Ke Wan & Singh, Manmeet Mahinderjit 2016. Wearable Technology Devices Security and Privacy Vulnerability Analysis. International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.3, May 2016. DOI: 10.5121/ijnsa.2016.8302.

Cho, Gilsoo 2010. Smart Clothing: Technology and Applications. < https://www.academia.edu/37239520/Smart_Clothing_Technology_and_Applications_Human_Factors_and_Ergonomics_Gilsoo_Cho_pdf>.

Cilliers, Liezel 2020. Wearable devices in healthcare: Privacy and information security issues. Health Information Management Journal (HEALTH INF MANAGE J), May-Sep2020; 49 (2/3). p. 150–156.

Comstock, Jonah 2015. Leaf Healthcare Gets $3.3M for Ulcer Prevention Wearable. <http://www.mobilehealthnews.com/46915/leaf-healthcare-gets-3-3m-for-ulcer-prevention-wearable>. Viitattu 3.5.2023.

Condeco 2018. The History of Wearable Technology. 14.9.2018. <condecosoftware.com/blog/the-history-of-wearable-technology/>. Viitattu 2.5.2023.

Cusack, Brian & Antony, Bryse & Ward, Gerard & Mody, Shaunak 2017. Assessment of security vulnerabilities in wearable devices. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. p. 42-48. DOI: 10.4225/75/5a84e6c295b44.

Datta, Prerit & Namin, Akbar Siami & Chatterjee, Moitrayee 2018. A Survey of Privacy Concerns in Wearable Devices. 2018 IEEE International Conference on Big Data (Big Data). DOI: 10.1109/BigData.2018.8622110.

Ericsson 2017. Wearable Technology and the IoT- Consumer Views on Wearables Beyond Health and Wellness. <https://www.ericsson.com/networked-society/trends-and-insights/consumerlab/consumer-insights/reports/wearable-technology-and-the-internet-of-things#wearablefuture>. Viitattu 2.5.2023.

Euroopan komissio 2024. < https://digital-strategy.ec.europa.eu/fi/policies/digital-services-act-package>. Viitattu 20.03.2024.

Ficom. <https://ficom.fi/ajankohtaista/uutiset/tietoturva-iot-ja-internet/>. Viitattu 29.01.2023.

Folk, Chris & Hurley, Dan C. & Kaplow, Wesley K. & Payne, James F. X. 2015. The security implications of the Internet of Things. AFCEA International Cyber Committee. <http://www.afcea.org/committees/cyber/documents/InternetofThingsF INAL.pdf> Viitattu 14.02.2023.

Grönlund, Mikko & Raitoharju, Reetta & Ranti, Tuomas & Seppälä, Kaapo & Ståhlberg, Tom 2017. Suomen terveysteknologia-alan nykytila ja haasteet. Tekes. Katsaus 340/2017. Helsinki.

Guler, Sibel Deren & Gannon, Madeline & Sicchio, Kate 2016. Crafting Wearables: Blending Technology with Fashion. Apress. <https://doi.org/10.1007/978-1-4842-1808-2>.

Handolin, Minna & Hämäläinen, Hannu 2022. Terveysdatan sujuva ja turvallinen käyttö- Viisi askelta kohti reilua datataloutta 2030. Sitran työpaperi. < https://www.sitra.fi/julkaisut/terveysdatan-sujuva-ja-turvallinen-kaytto/>.

Harenko, Kristiina & Niiranen, Valtteri & Tarkela, Pekka 2016. Tekijänoikeus. E-kirja. 2. uud. p. Helsinki: Talentum Pro, 2016.

Holstcentrewebinars.com 2020. Wearable health patches and Smart clothing for Vital Signs Monitoring and prevention of diseases.

<https://holstcentrewebinars.com/webinars/wearable-health-patches-for-remote-patient-monitoring-for-us-audience/>.

Hotus.fi; Joanna Briggs instituutin kriittisen arvioinnin tarkistuslistat. <https://www.hotus.fi/jbin-kriittisen-arvioinnin-tarkistuslistat/>. Viitattu 20.11.2023.

Härkönen, Tiina & Suomalainen, Kirsi & Vänskä, Riitta 2020. Ihmisistä kerätty data uppoaa monimutkaisiin verkostoihin. Sitran julkaisu. <https://www.sitra.fi/artikkelit/ihmisista-keratty-data-uppoaa-monimutkaisiin-verkostoihin/>.

Ioannidou, Irene & Sklavos, Nicolas 2021. On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. Cryptography 2021, 5(4), p. 29. DOI: 10.3390/cryptography5040029.

Iqbal, Mohammed & Aydin, Abdullatif & Brunckhorst, Oliver & Dasgupta, Prokar & Ahmed, Kamran 2016. “A review of wearable technology in medicine”. Journal of the Royal Society of Medicine Vol. 109 No. 10, p. 372–380. <https://journals.sagepub.com/doi/full/10. 1177/0141076816663560>.

Juutinen, Jukka-Pekka haastattelu 14.2.2022 & Keinonen Kalle 2022. EU tavoittelee uudella direktiivillä parempaa kyberturvaa. ItInsider. <https://itinsider.fi/eu-tavoittelee-uudella-direktiivilla-parempaa-kyberturvaa/>.

Jyväskylän yliopiston Koppa 2016. < https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/teemoittelu>. Viitattu 2.12.2023.

Kettunen, Salla & Joensuu-Salo, Sanna & Mäntysaari, Piia-Pauliina & Aalto, Anu & Marja Katajavirta 2020. Digitaalisuus muuttaa sosiaali- ja terveysalaa: osaamisen taso eteläpohjalaisissa pk-yrityksissä sekä esimerkkejä uudesta liiketoiminnasta. Seinäjoen ammattikorkeakoulun julkaisusarja B. Raportteja ja selvityksiä 150. Seinäjoki.

Khakurel, Jayden & Melkas, Helinä & Porras Jari 2018. Tapping into the wearable device revolution in the work environment: a systematic review. Information Technology & People Vol. 31 No.3, p. 791–818. <https://www.emerald.com/insight/content/doi/10.1108/ITP-03-2017-0076/full/html>.

Kosir, Spela 2015. Ten Sleep Wearable to Look for in 2015. <https://www.wearable-technologies.com/2015/05/ten-sleep-wearables-to-look-for-in-2015>. Viitattu 3.5.2023.

Kärkkäinen, Henrik 2015. Puettava teknologia muuttuu näkymättömäksi. Iltasanomat digitoday. 17.6.2015. <https://www.is.fi/digitoday/art-2000001878489.html>.

Kyngäs, Helvi & Elo, Satu & Pölkki, Tarja & Kääriäinen, Maria & Kanste, Outi 2011. Sisällönanalyysi suomalaisessa hoitotieteellisessä tutkimuksessa. Hoitotiede 23 (2), p. 138–148. Viitattu 24.5.2023.

Laaksonen, Anna-Maria 2020. Puettavilla älylaitteilla kerätty terveysdata – oikeudet ja hyödyntäminen. Pro Gradu- tutkielma, Lappeenrannan-Lahden teknillinen yliopisto LUT School of Business and Management. <https://lutpub.lut.fi/bitstream/handle/10024/161374/GRADU_Laaksonen.pdf;jsessionid=7D6D79C2D43862D7F7A3740C4AC9B8C8?sequence=1>.

Langley, Matthew R. 2015. Hide your health: Addressing the new privacy problem of consumer wearables. The Georgetown Law Journal, Vol. 103, p. 1641–1659.

Mahoney, Edward & Mahoney, Diane 2010. Acceptance of Wearable Technology by People With Alzheimer`s Disease: Issues and Accommodations. American Journal of Alzheimer`s Disease & Other Dementias Vol. 25 No. 6, 527–531.

Mediakasvatusseura 2019. Infograafi: Digitaalinen jalanjälki. Juliste. < https://mediakasvatus.fi/materiaali/infograafi-digitaalinen-jalanjalki/>.

Meola, Andrew 2016. Wearable Technology and IoT Wearable Devices. <http://www.businessinsider.com/wearable-technology-iot-devices-2016-8?r=US&IR=T&IR=T>. Viitattu 3.5.2023.

Miettinen, Markus 2002. Tietoturvan historiaa. Seminaari työ. Helsingin yliopisto. Tietojenkäsittelytieteen laitos.

Mikkonen, Eija 2013. Älylasit tuovat tietokoneen nenälle. <https://www.kaleva.fi/teemat/digi/alylasit-tuovat-tietokoneen-nenalle-katso-video-google-laseista/634972/>. Viitattu 8.5.2023.

Mills, Adam & Watson, Richard & Leyland, Pitt & Kietzmann, Jan 2016. Wearing safe: Physical and informational security in the age of the wearable device. Business Horizons, Vol. 59, Issue 6, November–December 2016, p. 615–622. DOI:org/10.1016/j.bushor.2016.08.003.

Mohsen, Toorani 2015. On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard. arXiv.org; Ithaca, Jan 12, 2015. DOI: 10.1007/978-3-662-48051-9_18.

Muurinen, Mika 2019. Tietosuoja vai tietoturva? Visma-blogi, julkaistu 27. tammik. 2019. <https://www.visma.fi/blog/tietosuoja-tietoturva/>.

Neittaanmäki, Pekka & Lehto, Martti & Savonen, Matti 2021. Yhteiskunnan digimurros. Jyväskylän yliopiston IT-tiedekunta. Yliopistopaino, Jyväskylä.

Niela-Vilén, Hannakaisa & Hamari, Lotta 2016. Kirjallisuuskatsauksen vaiheet. Teoksessa Stolt, Minna & Axelin, Anna & Suhonen, Riitta (toim.) Kirjallisuuskatsaus hoitotieteessä. Turun yliopisto. Hoitotieteen 34 laitoksen julkaisuja, tutkimuksia ja raportteja sarja A73. 2. korjattu painos. Helsinki: WSOYpro.

Nisonen, Mikko 2012. Tietoturvallisuuden hallintajärjestelmä Jyvsectec -hankkeeseen case: tietoturvan testausjärjestelmä. < https://www.theseus.fi/bitstream/handle/10024/52762/Nisonen_Mikko.pdf?sequence=1>.

Okonkwo, Chinedu & Awolusi, Ibukun & Nnaji, Chukwuma 2022. Privacy and security in the use of wearable internet of things for construction safety and health monitoring. IOP Conference Series: Earth and Environmental Science, Vol. 1101, W078: Information Technology for Construction. DOI: 10.1088/1755-1315/1101/9/092004.

Ometov, Alexandr & Shubina, Viktoriia & Klus, Lucie & Skibinska, Justyna & Saafi, Salva & Pascacio, Pavel & Flueratory, Laura & Gaibor, Darwin Quesada & Chukhno, Nadezhda & Chukhno, Olga & Ali, Asad & Channa, Asma & Svertoka, Ekaterina &

Qaim, Waleed Bin & Casanova-Marques, Raul & Holcer, Sylvia & Torres-Sospedra, Joaquin & Casteleyn, Sven & Ruggeri, Giuseppe & Araniti, Giuseppe & Burget, Radim & Hosek, Jiri & Lohan, Elena Simona 2021. A Survey on Wearable Technology: History, State-of-the-Art and Current Challence. Computer Networks 193. 108074.

Page, Matthew J. & McKenzie, Joanne E. & Bourtron, Isabelle & Hoffman, Tammy C. & Mulrow, Cynthia. 2020. The Prisma 2020 statement; an updated guideline for reporting systemic reviews. BMJ 2021;372:n71. Doi: 10.1136/bmj.n71. < http://prisma-statement.org/prismastatement/flowdiagram.aspx >. Viitattu 29.1.2024.

Park, Semi & Riha, Kim & Yoon, Hyunsik & Lee, Kyungho 2021. Hindawi, Volume 2021; Article ID 4973404. Data Privacy in Wearable IoT Devices: Anonymization and Deanonymization. DOI: 10.1155/2021/4973404.

Peker, Yeşem Kurt & Bello, Gabriel & Perez, Alfredo J. 2022. On the Security of Bluetooth Low Energy in Two Consumer Wearable Heart Rate Monitors/Sensing Devices. Sensors (Basel) 2022 Jan 27;22(3):988. DOI: 10.3390/s22030988.

Peters, Micah DJ & Godfrey, Christina & McInerney, Patricia & Munn, Zachary & Tricco, Andrea C & Khalil, Hanan 2020. JBI Manual for Evidence Synthesis. Chapter 11: Scoping reviews. <https://jbi-global-wiki.refined.site/space/MANUAL/4687342/Chapter+11%3A+Scoping+reviews>. Viitattu 1.12.2023.

Pormerleau, Mark 2015. Air Force Succesfully Tests Wearable Biometric Sensors. <https://gcn.com/articles/2015/10/06/biostamprc.aspx>. Viitattu 3.5.2023.

Quell 2017. 100% Drug Free Wearable Pain Relief Technology. <https://www.quellrelief.com/how-quell-works>. Viitattu 3.5.2023

Rajanen, Dorina & Weng, Min 2017. Digitization for fun or revard?: a study of acceptance of wearable devices for personal healthcare. Association for Computing Machinery, International Academic Mindtrek Conference, p. 154–159. Jultika.oulu.fi/Record/nbnfi-fe2018060125158. Viitattu 1.5.2023.

Rauttola, Ari-Pekka & Janne Halonen & Kristian Lukander & Tomi Passi & Arja Uusitalo & Saija Rauhamaa & Jussi Virkkala 2019. Puettavan teknologian hyödyntäminen työterveyshuolloissa ja työpaikoilla. Tampere: PunaMusta Oy. <https://www.julkari.fi/bitstream/handle/ 10024/139009/TTL-978-952-261-911-2.pdf?sequence=1>.

Reeder, Blaine & David, Alexandria 2016. Health at hand: A systematic review of smart watch uses for health and wellness. Journal of Biomedical Informatics Vol. 63, p. 269–276. <https://doi.org/10.1016/j.jbi.2016.09.001>.

Ryynänen, Tuomo 2016.Internet of Things selkokielellä. <https://blogit.haaga-helia.fi/ryynanen/2016/02/29/mita-internet-of-things-voi-tarkoittaa-selkokielella/> Viitattu 5.5.2023

Saaranen-Kauppinen, Anita & Puusniekka, Anna 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 25.5.2023.

Seneviratne, Suranga & Hu, Yining & Nguyen, Tham & Lan, Guohao & Khalifa, Sara & Thilakarathna, Kanchana & Hassan, Mahbub & Seneviratne, Aruna 2017. A survey of Wearable Devices and Challenges. IEEE Communications Surveys Tutorials Vol. 19 (4): p. 2573–2620. doi: 10.1109/COMST.2017.2731979.

Shukur, Fatina & Fatlawi, Ahmed 2022. Privacy and Security Awareness for Sensitive/Non-sensitive Data based Wearable Devices. Conference Paper. 2022 International Conference on Emerging Trends in Smart Technologies (ICETST).

Silva-Trujillo, Alejandra Guadalupe & González González, Mauricio Jacobo & Pérez, Luis Pablo Rocha & García Villalba, Luis Javier 2023. Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack. Sensors (Basel). 2023 Jun; 23(12): 5438. DOI: 10.3390/s23125438.

Srivastata, Bhavya 2014. Wearable Device Market Growth Will Decline After 2015: Healthcare and China Main Drivers! <https://dazeinfo.com/2014/06/03/wearable-device-market-growth-will-decline-2015-healthcare-china-main-drivers>. Viitattu 3.5.2023.

Stolt Minna & Axelin Anna & Suhonen Riitta 2016. Kirjallisuuskatsaus hoitotieteessä. Turun yliopiston julkaisuja.

TENK 2023. <https://tenk.fi/fi/tiedevilppi/hyva-tieteellinen-kaytanto-htk>. Viitattu 25.5.2023.

Traficom 2023. <https://www.tietoturvamerkki.fi/fi/alylaitteen-ostajalle>. Viitattu 25.5.2023.

Vaishnavi, A. R. & Sahana G & Guruprasad, N. 2023. Wearable Devices in the IoT: A Security and Privacy Perspective. Conference Paper. 2023 International Conference on IoT, Communication and Automation Technology (ICICAT).

Valtioneuvoston Luoti-julkaisu 2006. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78507/4_2006.pdf?sequence=1. Viitattu 10.1.2024.

Verronen, Pertti & Kaartinen Heidi & Nokela Sakari 2016. Tulevaisuuden Internet of Things (IoT) mittausympäristöt. Centria. <https://www.theseus.fi/handle/10024/104914>. Viitattu 5.5.2023.

Vähäkainu, Petri & Neittaanmäki, Pekka 2018. Digitaalinen terveys ja älykäs terveydenhuollon teknologia. Informaatioteknologian tiedekunnan julkaisuja no. 43/2018. <https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/digitaalinen-terveys-ja-alykas-terveydenhuollon-teknologia.pdf>.

Watts, Silvia 2016. The Internet of Things (IoT): Applications, Technology, and Privacy Issues. Nova Science Publishers.

Weber, Rolf. H. 2015. Internet of things: Privacy issues revisited. Computer Law & Security Review, Vol. 31 (5), p. 618–627.

Whiteman, Honor 2014. Wearable, Skin-like Device ´monitor cardiovascular`, Skin health 24/7. <http://www.medicalnewstoday.com/articles/283022.php> Viitattu 3.5.2023.

Yadav, Kumar & Mishra, Pragyan & Das Santos Kumar 2015. Study of Real-Time Miner Tracking Using Wireless Sensor Area Network. Internationa Conference on Microwawe, Optical and Communication Engineering, p. 330–333. Bhubaneswar.

Yli-Länttä, Asko 2021. Puettavan teknologian hyväksyminen terveydenhuollossa ja työpaikalla. <https://jyx.jyu.fi/bitstream/handle/123456789/74648/URN%3ANBN%3Afi%3Ajyu-202103161990.pdf?sequence=1&isAllowed=y>. Viitattu 20.03.2024.

Zhou, Wei & Piramuthu Selwyn 2014. Security/privacy of wearable fitness tracking IoT devices. Conference Paper. 9th Iberian Conference on Information Systems and Technologies (CISTI).

Liite 1 Katsaukseen valittu aineisto

Tekijät ja vuosiluku	**Tutkimusasetelma ja tutkimuksen tarkoitus**	**Tulokset**	**Laadun-arviointi pisteet ***
Arias, Orlando & Wurm, Jacob & Hoang, Khoa & Jin, Yier 2015	Tapaustutkimus Artikkelissa tarkastellaan IoT-laitteiden ja kannettavien älylaitteiden (wearable devices) suunnittelussa esiintyviä turvallisuusongelmia ja yksityisyyshaasteita. Lisäksi tarkastellaan kahden erityyppisen laitteen turvallisuutta: Nest-termostaatin ja Nike+ Fuelbandin, ja esitetään parannusehdotuksia tietoturvaan	-Melkein kaikki IoT- ja wearable-laitteet alkavat kerätä käyttäjätietoja asennuksesta lähtien -lait ja standardit määrittävät tietojen keräämistä, mutta osa niistä on osoittautunut tehottomiksi ja ne vanhentuvat nopeasti - suunnittelijat luottavat liikaa valmistajan tarjoamiin suunnitelmiin ja ratkaisuihin - avoin lähdekoodi vs. suljettu lähdekoodi -heikot tai virheelliset salausratkaisut -vianetsintärajapinnat tuotannon aikana ja toimitusketjun uhat - Nest thermostat: - ohjelmistopohjaiset suojaukset mahdollista ohittaa ja syöttää haitallista koodia - käynnistysprosessi altis manipuloinnille -etäpäivitysten heikko turvallisuus -kaikki kerätty data säilytetään laitteessa -hyökkääjät pystyivät saamaan pysyvän pääsyn laitteeseen - Nike+ Fuelband - flash-muistin sisältöön voi hyökätä -ei ole suojattu ulkoisilta luku- ja kirjoitusoperaatioilta -hyökkääjä pääsee laitteen vaihtoehtoiseen käynnistystilaan	Lista 1: 6/6

Tekijät ja vuosiluku	**Tutkimusasetelma ja tutkimuksen tarkoitus**	**Tulokset**	**Laadun-arviointi pisteet ***
Barua, Arup & Alamin, Abdullah Al. & Hossain, Shohrab & Hossain, Ekram 2022	Artikkeli Artikkelissa suoritetaan arviointi BLE-tietoturvaprotokollasta ja tunnistetaan sen tietoturvaan liittyviä haavoittuvuuksia, etenkin laitteiden pariliitoksiin liittyviä jotka aiheuttavat monia tietoturva- ja yksityisyysongelmia. Lisäksi luodaan luokitus erilaisista hyökkäysvektoreista ja esitellään erilaisia tekniikoita uhkien ehkäisyyn sekä tarjotaan suosituksia näiden uhkien lieventämiseksi.	-salauksen puute - paritusmenetelmien haavoittuvuudet -hyökkäykset, tietovuodot ja etäkoodin suoritus -sovelluskerroksen haavoittuvuudet tiedonkeruussa ja -jakamisessa -esimerkkinä SweynTooth-haavoittuvuudet ja Xiaomi Mi Bandin haavoittuvuudet	Lista 1: 6/6
Cai, Hang & Venkatasu-bramanian, Krishna K. 2018	Tapaustutkimus Tavoitteena oli kehittää menetelmä datan manipulointi -hyökkäysten havaitsemiseksi hyödyntäen fysiologisten sensorimittausten välistä yhteyttä sekä kuvarekonstruktioon perustuvaa luokittelijaa	-Riski: tietovuoto -Riski: laitteen tai datan manipulaatio sähkömagneettisen induktion, valon tai ääniaaltojen avulla -Riski: haittaohjelmat avoimien Bluetooth-porttien kautta -kehitetty menetelmä perustuu ajatukseen kuvantamisesta useiden samaa fysiologista prosessia mittaavien fysiologisten signaalien keskinäiseen suhteeseen, jolloin havaitaan yksipuolinen muutos yhdessä niistä olettaen, että toinen signaali ei ole muuttunut ja että sitä voidaan käyttää vertailukohtana -EKG-muutokset simuloitiin vaihtamalla mittaustuloksia ja menetelmän tarkkuus huomata tämä oli vähintään 98,23%. -menetelmä pystyy myös havaitsemaan verenpaineen mittauksissa tapahtuneet datan manipulointihyökkäykset 96,63% tarkkuudella -menetelmällä tulee myös vääriä hälytyksiä	Lista 1: 6/6

Tekijät ja vuosiluku	**Tutkimusasetelma ja tutkimuksen tarkoitus**	**Tulokset**	**Laadun-arviointi pisteet ***
Chikwetu, Lucy & Miao, Yu & Woldetensae , Melat K. & Bell, Diarra & Goldenholz, Daniel M. & Dunn, Jessilyn 2023	Katsaus Tässä katsauksessa pyrittiin selvittämään, voidaanko puettavista älylaitteista kerätystä datasta uudelleentunnistaa laitteen käyttäjä ja onko tiedon anonymisointi (deidentifying data) riittävä suojaamaan yksilöiden yksityisyyttä tietokantojen sisällä	-hyvin pienet datamäärät aiheuttavat yksityisyysriskin näennäisesti anonymisoidussa biosensoridatassa, oikeat identifikaatiotasot 86-100% -riski tietovuotoihin -riski palvelun käytön estämiseen -yritykset tekevät kolmannen osapuolen datanjakosopimuksia	Lista 2: 11/11
Chin, Ke Wan & Singh, Manmeet Mahinderjit 2016	Artikkeli Yleiskatsaus puettavien laitteiden tietoturva- ja yksityisyydensuojaa koskeviin haavoittuvuuksiin. Tehdään kolmelle puettavalle älylaitteelle tietoturva-analyysi	-puettavat älylaitteet eivät toimi yksinään vaan vaativat pariliitoksen esim. älypuhelimen kanssa useimpien toimintojen suorittamiseksi, BLE-suojauksen puute -Google Glass, Fitbit ja Samgsung- älykello olivat kaikki alttiita tietoturvaongelmille mm. epäturvallisen PIN-koodijärjestelmän tai heikon tunnistautumisen/valtuutuksen puutteen ja suojaamattoman verkon takia -Wi-Fi asennus QR-koodilla -käyttäjän sijainti voidaan jäljittää -tietojen tallennus paikallisesti ilman salausta -kuvia ja videoita voidaan tallentaa ilman käyttäjän lupaa -passiiviset ja aktiiviset hyökkäykset: -Brute force -hyökkäys -pilvessä mm. palvelunestohyökkäys -Man-in-the-middle-hyökkäys matkapuhelinverkon tai Wi-Fin kautta -laitteen pieni koko ja rajallinen kaistanleveys	Lista 1: 6/6

Tekijät ja vuosiluku	**Tutkimusasetelma ja tutkimuksen tarkoitus**	**Tulokset**	**Laadun-arviointi pisteet ***
		-Kehittäjät eivät aseta turvallisuutta ja yksityisyyttä etusijalle	
Cusack, Brian & Antony, Bryse & Ward, Gerard & Mody, Shaunak 2017	Poikkileikkaustutkimus Tutkimuksen tarkoitus oli selvittää, kuinka haavoittuvia puettavat älylaitteet ovat tietoturva- ja yksityisyyden suojan hyökkäyksille arvioimalla neljän 2016 markkinoita johtavan puettavan BLE-protokollaa langattomassa viestinnässä älypuhelimen kanssa käyttävää älylaitetta. Analyysiin valittiin Fitbit, Apple Watch, Amazon Fit ja Samsung Gear3 ja ne testattiin tietoturva-aukkojen löytämiseksi.	Kaikissa neljässä laitteessa oli tietoturvahaavoittuvuuksia: -suurin riski pariliitoksen aikana; man-in-the-middle-hyökkäykset, salakuuntelu, packet-injection, henkilöllisyys paljastui tekstinä -yksi laittteista paljasti pitkäaikaisen salausavaimensa selkokielisenä -laitteiden MAC-osoitteiden havaittiin olevan kiinteitä -salauksen puute, salattuihin tietoihin päästiin BLE-lokikirjan kautta, osassa BLE ei salattu -identiteettiuhka -brute-force-hyökkäykset -pakotettu uudelleen paritus -kerätyn tiedon omistajuus epäselvää -laitteen sijaintia pystyi seuraamaan - HCI (Human-Computer Interaction) Snoop Log, Bluetooth-protokollan osa, joka mahdollistaa tietokoneen ja Bluetooth-laitteen välisen kommunikoinnin, pystyi paljastamaan viestien lähettäjän henkilöllisyyden	Lista 3: 6/8
Datta, Prerit & Namin, Akbar Siami & Chatterjee, Moitrayee 2018	Katsaus Tarkastellaan puettavien älylaitteiden käyttöön liittyviä tietosuojahaasteita, esitellään jo olemassa olevia ratkaisuja, puhutaan avoimista kysymyksistä ja tulevaisuuden tutkimussuunnista	Riskit voidaan jakaa: tietojen keräämiseen, tietojen käsittelyyn, tietojen levittämiseen ja tunkeutumiseen - laitteet on suunniteltu olemaan jatkuvasti yhteydessä verkkoon, jolloin yhteys vuotaa tietoja -aika, paikka ja toiminto voidaan yhdistää fysiologisiin mittaustuloksiin ja tehdä päätelmiä käyttäjästä -fysiologisista mittaustuloksista voidaan tunnistaa yksilö.	Lista 2: 7/11

Tekijät ja vuosiluku	Tutkimusasetelma ja tutkimuksen tarkoitus	Tulokset	Laadun-arviointi pisteet *
		-tietovuodot, käyttäjän tietojen kerääminen ja prosessointi sekä datan eteenpäin jako. -puettavat älylaitteet, joissa on kamera, tallentavat myös sivullisia ilman heidän suostumustaan ja voivat paljastaa esim. sijainnin ja pankkiautomaattitapahtumat -käyttäjien tietämättömyys näistä riskeistä. -jotkut yritykset vastustavat laitteiden käyttöä tiloissaan; jäljityksen, turvallisuusuhkien, häiriötekijöiden ja arkaluontoisten tietojen tallentamisen pelko -maakohtaisten lakien ja säädösten yhtenäistäminen -lähes kaikki palvelut väittivät omistavansa käyttäjän terveystiedot. -ratkaisuja ongelmiin: standardointia, koulutusta ja tiedon lisäämistä.	
Ioannidou, Irene & Sklavos, Nicolas 2021	Tieteellinen artikkeli, jossa taustakatsaus ja kokeellinen analyysi Tavoitteena on tunnistaa yksityisyydensuoja- ja tietoturvariskit, joita käyttäjät voivat kohdata kuntoseurantasovellusten, älylaitteiden ja puettavan tekniikan käytössä sekä selvittää, onko tietosuoja ja turvallisuus vakiintunut puettaville laitteille uudella GDPR-aikakaudella? Kokeellinen analyysi suoritettiin valittuihin laitteisiin Man-in-the-middle-hyökkäyksen avulla	-kuntoilussa käytettävissä puettavissa älylaitteissa ja älykelloissa on merkittäviä tietoturvariskejä ja niiden sovelluksissa pyydetään laajoja oikeuksia -jaottelu: laitteisto-, ohjelmisto- ja verkkouhat -tietovuoto -standardoinnin puute -liitettävyys-, käsittely-, mediaseuranta- ja tallennustilan hallintaongelmat, linkittämisen ongelmat -hajautettu palvelunestohyökkäys (DDOS) -tietojen tahallinen muokkaus -sijainnin ennustaminen toimintohistorian avulla -sijainnin jakaminen	Lista 1: 5/6

Tekijät ja vuosiluku	Tutkimusasetelma ja tutkimuksen tarkoitus	Tulokset	Laadun-arviointi pisteet *
		-useat sovellukset eivät tarjoa asianmukaista tietosuojaa ja yritykset myyvät käyttäjätietoja kolmansille osapuolille ilman käyttäjän suostumusta -tietovuodot erityisesti Bluetooth- ja Wi-Fi-yhteyksien kautta -analysoidut sovellukset keräsivät sijainti- ja henkilökohtaisia tunnisteita ja muodostivat yhteyden Bluetoothin kautta ilman todennusta.	
Langley, Matthew R. 2015	Artikkeli -Puettavien älylaitteiden käytön yksityisyysongelmat ja kuinka kerättyjä tietoja voidaan edelleen käyttää -Analyysi laitteiden keräämien tietojen laajuudesta ja niiden vaikutuksista yksityisyyteen. -Arvioidaan voimassa olevaa lainsäädäntöä	-voimassa oleva lainsäädäntö, kuten HIPAA, ei koske kaupallisia laitteita eikä niiden keräämiä terveystietoja. Tällöin terveystietoja myydään kolmansille osapuolille ilman asianmukaista suojausta -sijaintia, poliittisia mieltymyksiä, yhteydenpitoa yhteyshenkilöihin, terveydentilaa koskevia hakukyselyjä ja monia muita arkaluonteisia tietoja kerätään ja myydään.	Lista 1: 6/6
Mills, Adam J. & Watson, Richard T. & Pitt, Leyland & Kietzmann, Jan 2016	Tieteellinen artikkeli Tässä artikkelissa käsitellään puettavien älylaitteiden tietoturvaa kolmesta näkökulmasta: onko uhka laitteelle ja/tai yksilölle, puettavan älylaitteen rooli ja miten laitteiden tietoturvastrategioita voidaan kehittää ja valvoa	-puettavat älylaitteet ovat henkilökohtaisempia muihin tietokoneisiin verrattuna -uhat laitteelle/käyttäjälle: -heikko tietoturva, tietomurto; arkaluontoisten tietojen vaarantaminen, anastaminen, tuhoaminen tai muuttaminen -tietovuoto käyttäjän paljastamiseksi tai laitteen tietojen manipulointi väärän tiedon välittämiseksi. -harhauttaminen, väärän tiedon jälkeisen toiminnan vaikutus käyttäjän hyvinvointiin -mahdollisuus aiheuttaa fyysistä haittaa käyttäjälle	Lista 1: 6/6

Tekijät ja vuosiluku	Tutkimusasetelma ja tutkimuksen tarkoitus	Tulokset	Laadun-arviointi pisteet *
		-laitteen toiminnan estäminen tai laitteen fyysinen vahingoittaminen, brute-force hyökkäys -vahvojen salasanojen puute -laitteen kautta mahdollista saada käyttäjän syntymäaika ja sosiaaliturvatunnus -yrityksille riski arkaluontoisiin tietoihin pääsystä -valmistajien kiire markkinoille tulossa tietoturvan kustannuksella -tietoturvastrategioiden ja lainsäädännän tarve	
Toorani, Mohsen 2015	Artikkeli Tavoitteena on arvioida turvallisuusnäkökohtia sekä suorittaa tietoturva-analyysi neljälle avaintenvaihtoprotokollalle, jotka ovat IEEE 802.15.6-standardoituja. Standardi käsittelee langattomia kehon alueverkkoja (Wireless Body Area Networks eli WBANs) haastamalla ne erilaisten hyökkäysten avulla.	Kaikilla neljällä protokollalla on turvallisuusongelmia. -haavoittuvia tehtyjä hyökkäyksiä vastaan eikä niissä ollut riittävää suojaa salauksen ja tunnistautumisen varmistamiseksi -haavoittuvia KCI-hyökkäykselle (Key-Compromise Impersonation), ja niiltä puuttuu PFS (perfect forward secrecy) -haavoittuvia imitaatiohyökkäykselle ja offline dictionary hyökkäykselle	Lista 1: 5/6
Okonkwo, C. & Awolusi, I. & Nnaji, C. 2022	Katsaus Katsauksessa tarkastellaan yksityisyyteen ja tietoturvaan liittyviä näkökohtia, turvallisuushaasteita, infrastruktuurivaatimuksia ja oikeudellisia kysymyksiä WIoT:n (wearable Internet of	-WIoT rakennusteollisuudessa altistuu samanlaisille turvallisuushyökkäyksille kuin IoT-laitteet muillakin aloilla: -anturisolmu-hyökkäys -luvaton RFID-pääsy -Man-in-the-middle-hyökkäys -univaje- hyökkäys	Lista 2: 8/11

Tekijät ja vuosiluku	Tutkimusasetelma ja tutkimuksen tarkoitus	Tulokset	Laadun-arviointi pisteet *
	Things) käytössä rakennusalalla. Lisäksi tarkastellaan yksityisyyden ja tietoturvan säädöksiä koskien turvallisuus- ja terveysdataa	-väärentäminen -haittaohjelmat -Sink hole- haavoittuvuus -tietojen kalastelu -järjestelmien tulisi täyttää vaatimukset tunnistautumisessa, anonymiteetissä, salauksessa ja liikenteen seurannassa. -Juridiset ja lain säädännälliset haasteet eri maissa	
Park, Semi & Riha, Kim & Yoon, Hyunsik & Lee, Kyungho 2011	Tapaustutkimus Miten piilotetun sijaintitiedon deanonymisointi voidaan suorittaa neljän skenaarion avulla keräämällä sijaintitiedot ja käsittelemällä ne uudestaan merkityksellisten tietojen aikaansaamiseksi ja kuinka tämä vaikuttaa käyttäjän yksityisyyteen ja tietoturvaan IoT-laitteissa.	-sijaintitietoja voidaan edelleen tunnistaa ja deanonymisoida, vaikka ne olisivat alun perin suojattu -puettavan älylaitteen kautta päästiin käyttäjän Google Maps-haun tuloksiin ja käyttäjän sijainti haun aikana saatiin selville -Wi-Fi-yhteyksiin liittyvistä lokitiedoista voidaan päätellä käyttäjän mahdollisia sijainteja kauppojen ja metroasemien SSID-nimien perusteella	Lista 1: 6/6
Peker, Yeşem Kurt & Bello, Gabriel & Perez, Alfredo J. 2022	Poikkileikkaustutkimus Analysoidaan kahta puettavaa älylaitetta ja yhtä näppäimistöä, jotka käyttävät Bluetooth Low Energy (BLE) -tekniikkaa. Tavoitteena on selvittää, mitkä BLE-standardien turvaominaisuudet on todella toteutettu näissä laitteissa	BLE-standardin mukaiset turvamekanismit eivät toteutuneet, vaan: -laitteita seurattiin, sillä osoitteita ei satunnaistettu, kiinteät MAC-osoitteet -käyttäjätiedot vaarantuivat, lähetetyt tiedot eivät olleet salattuja, tietovuoto -alhaiset suojaukset, brute force-hyökkäys onnistui -ei käyttäjän todennusta	Lista 3: 7/8

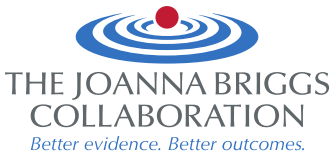
Liite 1

Tekijät ja vuosiluku	**Tutkimusasetelma ja tutkimuksen tarkoitus**	**Tulokset**	**Laadun-arviointi pisteet ***
Silva-Trujillo, Alejandra Guadalupe & González González, Mauricio Jacobo & Pérez, Luis Pablo Rocha & García Villalba, Luis Javier 2023	Poikkileikkaustutkimus Tutkimuksessa analysoidaan älykellojen tietoturvaa, erityisesti Bluetooth-yhteyksiin liittyvää turvallisuutta suorittamalla passiivinen hyökkäys kuuteen eri älykelloon paritusprosessin aikana	Kaikissa kuudessa älykellossa oli tietoturvaongelmia: -passiivinen tarkkailu/kuuntelu -man-in-the-middle -, offline-pin cracking- ja fuzzing-hyökkäykset -heikot paritusprotokollat -kiinteä MAC-osoite -kahdella kellolla ei todennusparia -tehty enimmäis- ja vähimmäisvaatimukset turvalliseen pariliitokseen	Lista 3: 8/8
Shukur, Fatina & Fatlawi, Ahmed 2022	Artikkeli Tarkoituksena on tutkia yksityisyyteen ja tietoturvaan liittyviä ongelmia puettavien laitteiden tietojen keräämisessä sekä lisätä käyttäjien tietoisuutta yksityisyyden ja tietoturvan merkityksestä. Lisäksi määritellään puettavien laitteiden ominaispiirteitä arkaluonteisten ja ei-arkaluonteisten tietojen osalta ja ehdotetaan puettavien laitteiden tietoturvaohjelmaa.	-jatkuva tallennus ilman käyttäjän suostumusta tai tietoisuutta -datan vuotaminen -hyökkäykset ja tunkeutuminen laitteeseen, tietomurrot -vanhusten ja lasten käyttämissä laitteissa tietoturvariskit ovat suuremmat tiedonpuutteesta johtuen	Lista 1: 6/6
Vaishnavi, A. R. & Sahana G &	Artikkeli Artikkeli käsittelee puettavan teknologian roolia IoT:ssa sekä siihen liittyviä	Haasteet: -tietosuoja -käytön hallinta ja todennus	Lista 1: 6/6

Tekijät ja vuosiluku	**Tutkimusasetelma ja tutkimuksen tarkoitus**	**Tulokset**	**Laadun-arviointi pisteet ***
Guruprasad, N. 2023	mahdollisuuksia ja haasteita sekä esittelee niihin ratkaisuehdotuksia	-tietovuoto -verkkojen turvallisuus	
Zhou, Wei & Piramuthu, Selwyn 2014	Artikkeli Tässä artikkelissa käsitellään puettavien kuntoiluseurantalaitteiden, erityisesti Fitbit-laitteen, tietoturvariskejä ja haavoittuvuuksia. Artikkeli perustuu Rahmanin ym. 2013 tekemään tutkimukseen, jossa tunnistettiin Fitbit-laitteen tietoturvaongelmia ja haavoittuvuuksia sekä ehdotettiin näiden ongelmien korjaustoimenpiteitä. Artikkeli pyrkii tarkastelemaan, kuinka hyvin ehdotetut korjaustoimenpiteet toimivat ja millaisia uusia riskejä ne voivat tuoda mukanaan.	-kuntoiluseurantalaitteen tunniste lähetetään selkokielisenä, jolloin laitetta voidaan seurata -passiiviset hyökkäykset -kuka tahansa voi liittää laitteen omaan tiliinsä	Lista 1: 5/6

*Lista 1= JBI Arviointikriteerit asiantuntijoiden näkemykselle ja narratiiviselle tekstille
Lista 2= JBI Arviointikriteerit järjestelmälliselle katsaukselle
Lista 3= JBI Arviointikriteerit poikkileikkaustutkimukselle

Liite 2 Aineiston luotettavuuden arvioinnissa käytetyt JBI tarkistuslistat



21.1.2019

JBI: Arviointikriteerit asiantuntijoiden näkemykselle ja narratiiviselle tekstille

Tätä tarkistuslistaa käytetään asiantuntijoiden näkemyksen ja narratiivisen tekstin metodologisen laadun arviointiin. Arvioinnin tarkistuslistaan sisältyy yhteensä 6 arviointikriteeriä joiden yksityiskohtaiset sisällöt on lyhyesti kuvattu alla. Arvioijan on hyvä tutustua myös Joanna Briggs Instituutin julkaisemaan katsauksen tekijöiden käsikirjaan arviointia tehdessään. Tarkistuslistan alkuperäinen englanninkielinen versio löytyy tästä linkistä. Kunkin kriteerin toteutuminen arvioidaan asteikolla: Kyllä (K), Ei (E), Epäselvä (?), Ei sovellettavissa (NA). (McArthur ym. 2015.)

Arvioija_____ Päiväys _____

Tekijä(t)_____ Vuosi _____ Nro _____

Arviointikriteeri	**K**	**E**	**?**	**NA**
1. Onko mielipiteen lähde selkeästi tunnistettavissa?	☐	☐	☐	☐
2. Onko mielipiteen lähteellä asema asiantuntijoiden joukossa?	☐	☐	☐	☐
3. Ovatko kohdeyleisön kiinnostuksen kohteet kirjoituksen keskiössä?	☐	☐	☐	☐
4. Onko esitetty näkemys analyyttisen prosessin tulos, ja onko esille tuodun mielipiteen taustalla logiikkaa?	☐	☐	☐	☐
5. Viitataanko olemassa olevaan kirjallisuuteen/näyttöön?	☐	☐	☐	☐
6. Puolustaako kirjoittaja näkemystään loogisesti suhteessa muuhun kirjallisuuteen tai lähteisiin?	☐	☐	☐	☐

Kokonaisarviointi: Hyväksy ☐ Hylkää ☐ Lisätietoja tarvitaan ☐

Kommentteja (mukaan lukien syy hylkäykseen):

_____

_____

Lähde: McArthur A, Klugarova J, Yan H, Florescu S. Innovations in the systematic review of text and opinion. Int J Evid Based Healthc. 2015;13(3):188–195.

29.11.2018

JBI: Arviointikriteerit järjestelmälliselle katsaukselle

Tätä tarkistuslistaa käytetään järjestelmällisen katsauksen metodologisen laadun arviointiin. Arvioinnin tarkistuslistaan sisältyy yhteensä 11 arviointikriteeriä, joiden yksityiskohtaiset sisällöt on lyhyesti kuvattu alhaalla. Arvioijan on hyvä tutustua myös Joanna Briggs Instituutin julkaisemaan katsauksen tekijöiden käsikirjaan arviointia tehdessään. Tarkistuslistan alkuperäinen englanninkielinen versio löytyy tästä linkistä. Kunkin kriteerin toteutuminen arvioidaan asteikolla: Kyllä (K), Ei (E), Epäselvä (?), Ei sovellettavissa (NA).

Arvioija_____ Päiväys _____

Tekijä(t)_____ Vuosi _____ Nro _____

Arviointikriteeri	**K**	**E**	**?**	**NA**
1. Onko katsauksen kysymys esitetty selvästi ja yksiselitteisesti?	☐	☐	☐	☐
2. Ovatko mukaanottokriteerit asianmukaiset verrattuna tutkimuskysymykseen?	☐	☐	☐	☐
3. Onko hakustrategia asianmukainen?	☐	☐	☐	☐
4. Ovatko käytetyt tiedonlähteet riittäviä?	☐	☐	☐	☐
5. Ovatko tutkimusten laadun arvioinnissa käytetyt kriteerit asianmukaiset?	☐	☐	☐	☐
6. Onko vähintään kaksi arvioijaa itsenäisesti toteuttanut tutkimusten kriittisen laadun arvioinnin?	☐	☐	☐	☐
7. Onko tietojen uuttamisvaiheessa käytetty menetelmiä virheiden minimoimiseksi?	☐	☐	☐	☐
8. Onko tutkimustulosten yhdistämisessä käytetty tarkoituksenmukaisia menetelmiä?	☐	☐	☐	☐
9. Onko katsauksessa arvioitu julkaisuharhan todennäköisyyttä?	☐	☐	☐	☐
10. Ovatko katsauksessa esitetyt käytännön suositukset linjassa katsauksen tulosten kanssa?	☐	☐	☐	☐
11. Ovatko katsauksessa esitetty jatkotutkimusehdotukset linjassa katsauksen tulosten kanssa?	☐	☐	☐	☐

Kokonaisarviointi: Hyväksy ☐ Hylkää ☐ Lisätietoja tarvitaan ☐

Kommentteja (mukaan lukien syy hylkäykseen):

THE JOANNA BRIGGS COLLABORATION
Better evidence. Better outcomes.

16.4.2019

JBI: Arviointikriteerit poikkileikkaustutkimukselle

Tätä tarkistuslistaa käytetään poikkileikkaustutkimuksen metodologisen laadun arviointiin ja tutkimuksen tuloksiin vaikuttavan mahdollisen harhan tunnistamiseen. Tarkistuslistaan sisältyy yhteensä 8 arviointikriteeriä, joiden yksityiskohtaiset sisällöt on kuvattu alhaalla. Arvioijan on hyvä tutustua myös Joanna Briggs Instituutin julkaisemaan katsauksen tekijöiden käsikirjaan arviointia tehdessään. Tarkistuslistan alkuperäinen englanninkielinen versio löytyy tästä linkistä. Kunkin kriteerin toteutuminen arvioidaan asteikolla: Kyllä (K), Ei (E), Epäselvä (?), Ei sovellettavissa (NA). (Moola ym. 2017.)

Arvioija_____ Päiväys _____

Tekijä(t)_____ Vuosi _____ Nro _____

Arviointikriteeri	**K**	**E**	**?**	**NA**
1. Onko otoksen mukaanotto- ja poissulkukriteerit määritelty selvästi?	☐	☐	☐	☐
2. Onko kohderyhmä ja tutkimusolosuhteet kuvattu riittävän tarkasti?	☐	☐	☐	☐
3. Mitattiinko altistus pätevästi ja luotettavasti?	☐	☐	☐	☐
4. Käytettiinkö objektiivisia, standardoituja kriteereitä osallistujien valintakriteerinä toimineen tilan/tilanteen mittaamiseen?	☐	☐	☐	☐
5. Onko sekoittavat tekijät tunnistettu?	☐	☐	☐	☐
6. Mainitaanko menetelmät, joita käytettiin sekoittavien tekijöiden huomioimisessa?	☐	☐	☐	☐
7. Onko tulosmuuttujat mitattu pätevästi ja luotettavasti?	☐	☐	☐	☐
8. Käytettiinkö soveltuvia tilastollisia menetelmiä?	☐	☐	☐	☐

Kokonaisarviointi: Hyväksy ☐ Hylkää ☐ Lisätietoja tarvitaan ☐

Kommentteja (mukaan lukien syy hylkäykseen):

_____

_____