Sanni Teukku

ESINEIDEN INTERNETIN HYÖDYT YKSILÖLLE TURVALLISUUDEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Teukku, Sanni
Esineiden internetin hyödyt yksilölle turvallisuuden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2017, 29 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Koskelainen, Tiina

Tässä tutkielmassa esitellään esineiden internetin hyötyjä yksilölle turvallisuuden näkökulmasta. Aihe on tärkeä, sillä esineiden internet on nopeasti ja jatkuvalla tahdilla kasvava ilmiö, joka tulee väistämättä vaikuttamaan huomattavasti nykyiseen ja tulevaan yhteiskuntaan. Kehittyvien teknologioiden ansiosta lähitulevaisuudessa lähes jokainen esine voidaan yhdistää internetiin, mikä mahdollistaa valtavan potentiaalin esineiden internetin hyödyntämiselle. Tutkielmassa keskitytään esineiden internetin mahdollistamiin yksilön turvallisuushyötyihin. Tutkimuskysymyksenä on mitä eri turvallisuushyötyjä yksilö saa esineiden internetistä ja miten ne parantavat yksilön turvallisuutta. Tutkielmassa turvallisuushyötyjä tarkastellaan neljästä näkökulmasta: turvallisuushyödyt liikenteessä, terveydenhuollossa, kotona ja yksilön henkilökohtaiset turvallisuushyödyt. Tutkielmassa huomioidaan myös esineiden internetin ongelmat, kuten ongelmat yksityisyyden suojaamisessa ja tietoturvassa. Tutkielma on tehty kirjallisuuskatsauksena ja aineisto tutkielmaa varten on kerätty pääasiassa IEEE Xplore ja Google Scholar –hakukoneilla sekä Jyväskylän yliopiston kirjaston tietokannasta. Tutkielmassa esitellään kattava määrä erilaisia turvallisuushyötyjä yksilölle ja kerrotaan miten eri hyödyt vaikuttavat yksilön turvallisuuteen. Tutkielmassa selvisi että saavutetut hyödyt toteutuvat pääasiassa neljällä tavalla. Nämä neljä tapaa ovat tietojen kerääminen, tietojen analysointi, tiedon välitys esineiden välillä ja esineiden välittämä tieto yksilölle. Näiden avulla yksilö saa arvokasta tietoa turvallisuuden kannalta sekä itsestään että ympäristöstään. Lisäksi yksilö voi tehdä turvallisuuttaan tukevia päätöksiä esineiden internetin avulla saamiensa tietojen perusteella tai luottaa siihen, että esineet osaavat toimia itsenäisesti yksilön parhaaksi. Parhaimman hyödyn esineiden internetistä saadaan, kun jokaista neljää tapaa käytetään yhdessä.

Asiasanat: esineiden internet, turvallisuus, RFID, sensorit, langattomat sensoriverkot, yksilö

ABSTRACT

Teukku, Sanni
The benefits of the Internet of Things to the individual from a security point of view
Jyväskylä: University of Jyväskylä, 2017, 24 p.
Information Systems, Bachelor's Thesis
Supervisor: Koskelainen, Tiina

This thesis presents the benefits of the Internet of Things to the individual from a security point of view. The subject is important because the Internet of Things is a rapidly growing phenomenon that will inevitably have a significant impact on current and future societies. With the advancement of emerging technologies in the near future, almost every item can be connected to the internet, enabling enormous potential. The purpose of this thesis is to answer the question of what kind of different benefits individual can get from the Internet of Things and how will the benefits improve the security of the individual. In this thesis, safety benefits are examined from four perspectives: safety benefits in traffic, health care, home and individual's personal safety benefits. The thesis also takes into account safety issues related to the Internet of Things, such as information security and privacy issues. This thesis is a literature review and the material for the thesis was mainly collected from IEEE Xplore and Google Scholar search engines and also from the Jyväskylä University library's database. The thesis presents a comprehensive range of safety benefits to the individual and explains how the various benefits affect the safety of the individual. The thesis found that the benefits achieved can be presented in four categories. These are data gathering, analyzing data, communication between objects, and communication to the individual. By doing this, the individual gets valuable information about security both from oneself and from the environment. In addition, an individual can make security-based decisions based on the information individual have acquired from the Internet, or rely on things to act independently for the best of the individual.

Keywords: internet of things, safety, RFID, sensors, wireless sensor network, individual

TAULUKOT

SISÄLLYS

1 JOHDANTO

Esineiden internet on miljardien keskenään vuorovaikutuksessa olevien laitteiden verkko ja se on merkittävässä osassa tietotekniikan ja viestinnän kehityksessä tulevina vuosikymmeninä. (Atzori, Iera & Morabito, 2010; Buckley, 2006.) Al-Fuqahan, Guizanin, Mohammadin, Aledharin ja Ayyashin (2015) mukaan esineiden internet antaa erilaisille fyysisille esineille kyvyn nähdä, kuulla, ajatella, vaihtaa tietoja keskenään ja näin toimia yhdessä. Gartner (2017) arvioi että vuonna 2017 maailmassa tulisi olemaan 8,4 miljardia internettiin kytkettyä laitetta ja ennustaa määrän nousevan yli 20 miljardiin vuonna 2020. Viimeisimmät kehitysaskeleet radiotaajuisessa etätunnistuksessa, sensoreissa, viestintäteknologioissa ja internet-protokollissa ovat mahdollistaneet esineiden internetin nykyisen kasvun (Al-Fuqaha ym., 2015). Yhä useampi esine on siis etenevässä määrin kykenevä havainnoimaan ympäristönsä muutoksia ja reagoimaan niihin itsenäisesti.

Yksi esineiden internetin suurimpia vahvuuksia tulee olemaan sen aiheuttama vaikutus jokapäiväiseen elämään. Yksilön kannalta suurimmat vaikutukset näkyvät sekä työelämässä että kotitalouksissa. (Atzori ym., 2010.) Esimerkiksi tuettu asuminen, terveys sekä liikenne ovat alueita, joissa esineiden internetin uskotaan hyödyntävän yksilöä (Xia, Yang, Wang & Vinel, 2012). Gartnerin (2017) mukaan kuluttajat kattavat 63 % koko esineiden internetin käyttäjäkunnasta ja ovat siten suurin yksittäinen käyttäjäryhmä.

Tutkielmassa keskitytään esineiden internetin hyötyihin yksilölle turvallisuuden näkökulmasta. Esineiden internetin erilaisista ongelmista ja haasteista yksilön näkökulmasta on kirjoitettu paljon, mutta hyötyjen kertominen, erityisesti turvallisuuden näkökulmasta, on jäänyt vähemmälle. Tutkimuskysymyksenä on mitä eri turvallisuushyötyjä yksilö saa esineiden internetistä ja miten ne parantavat yksilön turvallisuutta. Tutkielmassa yksilön turvallisuudella tarkoitetaan tilaa, jossa yksilö ei ole välittömässä vaarassa ja yksilöllä on kyky hallita parhaansa mukaan mahdollisia nykyisiä ja tulevia uhkatilanteita.

Tutkielman tarkoituksena on siis tuoda esille ensisijaisesti esineiden internetin turvallisuushyötyjä. Aiheen tutkiminen on tärkeää, sillä esineiden internetin järkevällä hyödyntämisellä voidaan lisätä merkittävästi yksilön turvallisuutta.

Tutkielmassa esitetyt esineiden internetin hyödyt voidaan jakaa ominaisuuksiensa perusteella neljään osa-alueeseen, jotka ovat tietojen kerääminen, tietojen analysointi, tiedon välitys esineiden välillä ja esineiden välittämä tieto yksilölle. Ensinnäkin esineiden internetin keräämän tiedon perusteella yksilö saa tarkemman ja kattavamman kuvan omasta elämästään ja siihen vaikuttavista asioista. Analysointi puolestaan mahdollistaa yksilölle älykkäämpiä ratkaisuja turvallisuusongelmiin. Esineiden internetillä on valtava määrä yksilöstä kerättyä tietoa, jonka ansiosta esineet kykenevät suodattamaan yksilön turvallisuuden kannalta keskeisimmät tiedot ja jättää epäolennaiset huomioimatta. Kolmanneksi, kommunikoimalla muiden esineiden kanssa esineet saavat tarkemman kokonaiskuvan kustakin vallitsevasta tilanteesta. Viimeisenä on tiedon välittäminen yksilölle, mikä mahdollistaa muun muassa yksilön tiedottamisen ja varoittamisen.

Atzor ym. (2010) esittelevät tutkimuksessaan esineiden internetin hyötyjä. He ovat jakaneet hyötyjen perusteella neljä käyttökohdetta, joissa esineiden internetiä pääsääntöisesti hyödynnetään (2793). Nämä käyttökohteet ovat:

- Kuljetus ja logistiikka
- Terveydenhuolto
- Älykkäät ympäristöt (koti, toimisto, tehtaat)
- Yksityiselämä

Tutkielmassa keskitytään yksilön turvallisuuteen näistä neljästä käyttökohteesta esittäen jo olemassa olevia tai lähitulevaisuudessa laajempaan käyttöön todennäköisesti tulevia hyötyjä. Koska tutkielmassa esiteltyjen hyötyjen pääsääntöisenä tarkoituksena on lisätä yksilön turvallisuutta, on tutkielmasta jätetty pois turvallisuuteen liittymättömät hyödyt sekä sellaiset hyödyt, jotka eivät kohdistu nimenoman yksilöön. Älykkäiden ympäristöjen osalta näkökulma on rajattu kotiin, sillä ihminen viettää suuren osan päivästään kotona ja monelle koti on tärkein paikka elämässä.

Tutkielma tehtiin kirjallisuuskatsauksena. Aineistoa kerättiin pääasiassa IEEE Xplore ja Google Scholar –hakukoneilla. Lisäksi tietoa haettiin Jyväskylän yliopiston kirjaston tietokannasta ja keskeisten artikkeleiden lähdeluetteloista. Hakusanoina käytettiin muun muassa seuraavia sanoja tai niiden yhdistelmiä: internet of things, security, safety, radio frequency identification, wireless sensor networks, sensors, personal, benefits, healthcare, smart cars, smart homes, esineiden internet, turvallisuus, yksilön turvallisuus.

Tutkielman rakenne koostuu johdannosta, kolmesta sisältöluvusta ja yhteenvedosta. Ensimmäisessä sisältöluvussa kerrotaan mitä käsite esineiden internet tarkoittaa, miten se on kehittynyt ja mitkä ovat esineiden internetin keskeiset toimintaperiaatteet. Toisessa sisältöluvussa kerrotaan yleisellä tasolla mitä turvallisuudella tarkoitetaan, mitä on yksilön turvallisuus ja miten esineiden internet voi vaikuttaa turvallisuuteen. Lisäksi toisessa sisältöluvussa kerrotaan esineiden internetin turvallisuusongelmista. Kolmannessa sisältöluvussa esitellään tarkemmin esineiden internetin hyötyjä yksilölle jo esitellystä neljästä

käyttökohteesta: esineiden internetin hyödyt yksilölle liikenteessä, terveydenhuollossa, kotona ja henkilökohtaisessa elämässä. Lopuksi yhteenvedossa kerrataan tulokset ja esitetään huomioita tuloksista.

2 ESINEIDEN INTERNET

Esineiden internetille ei ole olemassa yhtä sovittua yleistä määritelmää. Useat kirjoittajat tuntuvat kuitenkin olevan yhtä mieltä esineiden internetin ydinajatuksesta (Atzori ym., 2010; Collin & Saarelainen, 2016; Rose, Eldridge & Chapin, 2015; Tozlu, Senel, Mao & Keshavarzian, 2012; Whitmore, Agarwal & Da Xu, 2015), joka on että erilaiset ympärillämme olevat esineet ovat liitettävissä internetiin ja internetin avulla esineet alinomaan välittävät, tallentavat ja analysoivat keräämäänsä informaatiota reaaliajassa. Lisäksi esineet ovat yksilöitävissä ja kykenevät välittämään tietoa toisilleen. Esineet varustetaan erilaisilla sensoreilla, toimilaitteilla ja tunnisteilla, joiden avulla esineet havainnoivat ja keräävät tietoa ympäristöstään. Esineet voivat olla mitä tahansa jokapäiväisiä esineitä aina ajoneuvoista lääkinnällisiin tarvikkeisiin. Tiedon välittämiseen esineet käyttävät muun muassa radiotaajuista etätunnistamista, langattomia sensoriverkkoja ja mobiiliverkkoja (Atzori ym., 2010). Näin esineet voivat vaihtaa tietoa keskenään ja toimia älykkäästi yhdessä esimerkiksi varoittaakseen ihmistä mahdollisesta vaarasta.

2.1 Kehitys kohti esineiden internetiä

Internet on jatkuvasti kehittyvä kokonaisuus, jonka merkitys ja hyötykäyttö lisääntyvät koko ajan (Coetzee & Eksteen, 2011). Internet on ollut olemassa yli 50 vuotta ja sinä aikana se on kasvanut pienestä tutkijoiden käyttöön tarkoitetusta tietoverkosta maailmanlaajuiseksi verkoksi (Kopetz, 2011). Tänä päivänä internetillä on miljardeja käyttäjiä ja 40 %:lla maailman väestöstä on pääsy internetiin (Internet Live Stats). Määrä tulee kasvamaan jatkuvasti kun yhä useammalla yksilöllä on pääsy internetiin teknologian ja internetyhteyksien halventuessa. Viime vuosien aikana internet on muuttunut yhä enemmän ihmisen internetiksi, luoden sellaisia käsitteitä kuin sosiaalinen verkko, jossa ihmiset aktiivisesti luovat ja käyttävät internetin sisältöä (Coetzee & Eksteen, 2011). Internetin kehittyminen ja yleistyminen on johtanut ihmisten yhdistymiseen odot-

tamattomalla laajuudella ja tahdilla. Gubbi, Buyya, Marusic ja Palaniswami, (2013) esittävät että seuraava vallankumous tulee olemaan toisiinsa ja internetiin yhdistyneet laitteet, jotka luovat älykkään ympäristön.

Tätä vallankumousväitettä tukee teknologian kehitys, mikä on laajentanut internetin käyttömahdollisuuksia. Samalla kun teknologian kehittyminen tekee laitteista yhä pienempiä, niiden käsittelyteho ja muistikapasiteetti kasvavat mahdollistaen monipuolisempien esineiden pääsyn internetiin. Erilaisiin esineisiin upotetaan yhä enemmän sensoreita, toimilaitteita ja internetyhteyden mahdollistavia teknologioita. Nämä antavat laitteille kyvyn aistia, laskea ja toimia itsenäisesti, sekä internetyhteyden avulla olla osa internetiä. (Coetzee & Eksteen, 2011; Tuwanut & Kraijak, 2015.)

Laitteiden osien kustannusten aleneminen ja uusien valmistusmenetelmien, kuten tulostettavan elektroniikan, hyödyntäminen mahdollistavat esineiden internetin teknologioiden laajenemisen osaksi arjen esineitä. Esineiden internetin kasvua lisäävät myös pilvipalvelut ja matkapuhelinstandardit, jotka mahdollistavat entistä sujuvamman langattoman tiedonsiirron. (Jurvansuu & Belloni, 2013.) Ihmiset käyttävät yhä enemmän langattomia älylaitteita arjessaan, kuten älypuhelimia, tabletteja ja kannettavia tietokoneita. Lisäksi laajakaistayhteydet ovat yhä halvempia ja useamman saatavilla, myös kehittyvissä maissa. (Coetzee & Eksteen, 2011.) Kaikki edellä mainitut osatekijät mahdollistavat sen, että kuilu fyysisen maailman ja verkkoavaruuden välillä tulee pienentymään ja internetin käsite laajenee kohti esineiden internetiä (Tuwanut & Kraijak, 2015).

Internet ja teknologioiden kehittyminen yhdessä mahdollistavat jokapäiväisten esineiden muuttamisen älykkäiksi esineiksi, jotka ymmärtävät ja reagoivat ympäristöönsä (Kortuem, Kawsar, Fitton & Sundramoorthy, 2010). Myös jokapäiväiset esineet, joita ei ole aikaisemmin pidetty elektronisina, ovat nyt entistä enemmän verkossa sensoreiden ja mikroprosessorien avulla. Tähän sisältyy esineitä kuten kauppojen tuotteet, vaatteet, kodinkoneet, erilaiset hyödykkeet sekä rakennukset ja tiet. (Swan, 2012.)

Buckleyn (2006) mukaan esineiden internetiin kuuluvilla laitteilla on neljä kehittyneisyyden tasoa. Ensimmäisellä tasolla on puhtaasti passiiviset laitteet, jotka toimivat radiotaajuisen etätunnistuksen avulla ja jotka antavat pyydettäessä tietyn ennalta määrätyn informaation. Toisella tasolla ovat laitteet, joilla on kohtalainen laskentateho välittää tietoa ja ne voivat muokata välittämänsä informaation sisältöä ajan ja paikan mukaan. Kolmannella tasolla ovat havainnoivat laitteet, jotka tuottavat ja lähettävät tietoa ympäristöstään, esimerkiksi paineesta, lämpötilasta, valon määrästä ja sijainnista. Neljännellä ja kehittyneimmällä tasolla on laiteet, jotka pystyvät olemaan itsenäisesti vuorovaikutuksessa toisen laitteen kanssa ilman käyttäjän tekemää erillistä pyyntöä. (Buckley, 2006.)

2.2 Esineiden internetin toimintalogiikka

Esineiden internet mahdollistaa erilaisille esineille kyvyn havainnoida ympäristöään, kerätä tietoa, olemaan yksilöitävissä, välittämään tietoa ja mahdollisuuden internetyhteyteen. Seuraavissa luvuissa kerrotaan tarkemmin esineiden internetin toiminnan mahdollistavista teknologioista ja yleisesti toimintalogiikasta.

2.2.1 Radiotaajuinen etätunnistus, RFID

Radiotaajuinen etätunnistus (englanniksi Radio Frequency Identification, RFID) on yksi tärkeimmistä esineiden internetin mahdollistavista teknologioista. Radiotaajuinen etätunnistus on lyhyen kantaman tiedonvälitysteknologia, joka koostuu RFID-tunnisteista ja niitä lukevista RFID-lukijoista (Whitmore ym., 2015.) RFID-tunnisteet koostuvat mikrosirusta ja antennista. Tunnisteet on suunniteltu tiedon tallentamiseen ja langattomaan tiedonsiirtoon. Mikrosiru, joka voi olla yhtä pieni kuin hiekanjyvä, sisältää esineen tietoja, kuten yksilöllisen tunnistenumeron. Antenni puolestaan mahdollistaa tiedonvälityksen tunnisteen ja RFID-lukijan välillä. RFID-tunnisteen avulla voidaan seurata ja tunnistaa esineitä ja ihmisiä, joihin RFID-tunniste on kiinnitetty. (Juels, 2006).

RFID-lukija lukee RFID-tunnisteeseen tallennettuja tietoja radiotaajuisten sähkömagneettisten kenttien avulla (Whitmore ym., 2015). RFID-tunnisteet sisältävät laitteen yksilöllisen tunnistusnumeron, jonka avulla RFID-lukija pystyy identifioimaan jokaisen RFID-tunnisteen. Tunnisteet voivat lisäksi sisältää muutakin informaatiota, kuten tiedon valmistajasta, tai ne voivat jopa mitata ja tallentaa tietoja ympäristöstään, kuten tiedon ilman lämpötilasta. (Want, 2006). Identifioimista ja tiedonsiirtoa varten RFID-lukijalla ei tarvitse olla suoraa näköyhteyttä tunnisteeseen vaan riittää että lukija on samassa tilassa. RFID-lukija voi myös lukea useita tunnisteita kerralla ja automaattisesti. (Want, 2004). RFID-tunnisteita voidaan seurata tarvittaessa maailmanlaajuisesti, automaattisesti ja reaaliajassa.

RFID-tunnisteet jaetaan passiivisiin ja aktiivisiin. Aktiiviset tunnisteet tarvitsevat oman virtalähteen, kuten patterin, jonka takia ne ovat kalliimpia kuin passiiviset. Aktiiveissa tunnisteissa on isompi tallennustila ja ne voivat sisältää sensoreita, jotka mittaavat ympäristöä. Aktiivisten tunnisteiden tietoja voidaan lukea RFID-lukijalla kauempaa kuin passiivisten tunnisteiden. (Kopetz, 2011; Want, 2006.) Lisäksi aktiiviset tunnisteet voivat kommunikoida muiden RFID-tunnisteiden kanssa ja ne voivat välittää tietoa RFID-lukijalle itsenäisesti ilman ihmisen erillistä käskyä (Jia, Feng, Fan & Lei, 2012). Passiiviset tunnisteet puolestaan eivät tarvitse omaa virtalähdettä, sillä ne saavat virtansa RFID-lukijasta (Jia ym., 2012). Koska passiiviset tunnisteet eivät tarvitse omaa virtalähdettä, ne kestävät käytössä vuosia ja ovat tarpeeksi pieniä, jotta niitä voidaan käyttää esimerkiksi tuotteeseen liimattavassa etiketissä (Want, 2006). Tämä mahdollistaa niiden monipuolisemman käytön verrattuna aktiivisiin tunnisteisiin.

Sundmaekerin ym. (2010) mukaan RFID-teknologian hyödyntämistä on hidastanut erilaiset tekijät, kuten RFID-tunnisteiden kallis hinta verrattuna perinteiseen viivakoodiin ja huolet yksityisyyden takaamisessa. Toisaalta, Kopetz (2011) sanoo artikkelissaan, että RFID-teknologian standardisointi ja RFID-teknologian kehittyminen on alentanut RFID-tunnisteiden kustannuksia huomattavasti viime vuosina, mikä edesauttaa RFID-teknologian hyödyntämistä. Eriävistä näkemyksistä huolimatta voidaan kuitenkin sanoa, että RFID-teknologian hyödyntäminen on kasvussa. Yksi syy siihen on RFID-tunnisteisen esineen mahdollisuus liikuteltavuuteen, sillä samanlainen vapaa liikuteltavuus ei ole mahdollista langallisilla laitteilla (Buckley, 2006). Liikuteltavuuden lisäksi RFID-teknologian suosion kasvuun vaikuttaa RFID-teknologian monipuolinen hyödyntäminen. RFID-teknologiaa voidaan hyödyntää erittäin laajasti eri osa-alueilla, kuten logistiikassa, terveydenhuollossa ja kotien turvallisuudessa (Atzori ym., 2010).

2.2.2 Sensorit ja langattomat sensoriverkot

Sensorit ovat laitteita, jotka tekevät havaintoja ja tarkkailevat ympäristöään tai muiden esineiden ominaisuuksia. Sensorit voivat havainnoida ympäristöstään esimerkiksi lämpötilaa, ilman kosteutta ja valon määrää. Vastaavasti esineestä, johon sensori on kiinnitetty, sensori voi havainnoida esimerkiksi esineen kokoa, liikkumisnopeutta ja esineen sijainnin. (Whitmore ym., 2015; Zheng & Jamalipour, 2009.) Sensorit keräävät informaatiota reaaliajassa kaikkialla, koko ajan ja kaikissa tilanteissa. Sensorit voivat lähettää kerätyn informaation eteenpäin erilaisilla viestintätekniikoilla kuten matkapuhelinverkon, Bluetoothin tai Wi-Fin välityksellä. (Gupta & Gupta, 2016.)

Sensorit voivat myös muodostaa langattomia sensoriverkkoja (englanniksi wireless sensor networks, WSN), joissa useat sensorit toimivat yhdessä ja välittävät tietoa toisilleen (Whitmore ym., 2015). Sensoriverkon sensorit ovat pieniä, ne ovat halpoja verrattuna tavallisiin sensoreihin ja niillä on rajallinen prosessointi- ja laskentateho. Sensoriverkossa sensoreita voi olla muutamasta kymmenestä sensorista aina tuhansiin. Sensoriverkon sensoreiden tarkoituksena on kerätä tietoa ympäristöstä, toimia yhdessä ja välittää tietoa sekä toisille sensoriverkon sensoreille, että sensoriverkon ylläpitäjälle. (Yick, Mukherjee & Ghosal, 2008.)

Toimilaitteita käytetään usein sensoreiden kanssa yhdessä, jolloin ne muodostavat sensori-toimilaite-verkon. Sensorit havainnoivat ympäristön tai esineen tilaa, kun toimilaitteet taas suorittavat toimintoja, jotka vaikuttavat ympäristöön tai esineeseen jollakin tavoin. Toimilaitteet voivat vaikuttaa ympäristöön esimerkiksi tuottamalla ääntä, valoa, radioaaltoja tai jopa tuoksuja. Yksi esimerkki tällaisesta toimilaitteen käytöstä voisi olla seuraava: sensori havaitsee huoneessa olevan myrkyllistä hiilimonoksidia eli häkää, jolloin sensorin tieto välittyy toimilaitteelle, joka päästää ilmoille kovan hälytyksen ja varoittaa huoneessa olijoita. (Whitmore ym., 2015.)

3 TURVALLISUUS

Turvallisuudelle ei ole yksiselitteistä määritelmää. Kielitoimiston sanakirjan mukaan sana ”turvallinen” tarkoittaa jotakin, jossa ei ole vaaraa, mikä on suojainen, vaaraa aiheuttamaton eli käytännössä vaaraton. Turvallisella tarkoitetaan myös luotettavaa, kokemusta turvallisuuden tunteesta ja luottamuksesta. Sanastokeskus ja Suomen Pelastusalan Keskusjärjestö (2014) määrittelevät kokonaisturvallisuuden sanastossaan turvallisuuden tilana ja toimintoina jolloin uhkat ja riskit ovat hallittavissa. Tässä tutkielmassa turvallisuudella tarkoitetaan tilaa, jossa yksilö ei ole välittömässä vaarassa ja yksilöllä on keinoja turvallisuutta uhkaavien tekijöiden hallintaan.

3.1 Yksilön turvallisuus ja turvallisuus esineiden internetissä

Maslow (1987) kirjoittaa turvallisuudesta yksilön perustarpeena. Maslow’n klassisessa tarvehierarkiassa turvallisuus on tärkeysjärjestyksessä heti toisena fysiologisten tarpeiden jälkeen. Fysiologisilla tarpeilla tarkoitetaan tarpeita, joilla ihminen pysyy hengissä, kuten ruoka ja vesi. Kun nämä tarpeet on tyydytetty, ihminen alkaa luontaisesti etsiä turvallisuutta. Maslow määrittelee turvallisuuden kolmesta näkökulmasta. Ensinnäkin vakautena, luottamuksena ja suojana. Toisena vapautena pelosta, ahdistuksesta ja kaaoksesta. Viimeisenä Maslow’n mukaan turvallisuus tarkoittaa halua järjestykselle, laille ja rajoille. (Maslow, 1987). Puolustusministeriö (2007) määrittelee turvallisuustoiminnan strategiassaan, että yksilölle turvallisuus on tarve ja tunne, joihin vaikuttavat sekä yksilön ympärillä vallitseva tilanne, että yksilön oma tulkinta vallitsevasta tilanteesta. Tämän mukaan siis esimerkiksi valtiossa vallitseva rauha ei välttämättä yksinään takaa yksilön kokemusta turvallisuudesta. Samaan päätelmään on päätynyt myös Sipponen (1990), joka kirjoittaa että yksilölle turvallisuus ei ole pelkästään turvallisen valtion, asevoimien tai yhteiskunnan diplomatian olemassaoloa, vaan näiden lisäksi yksilön henkilökohtaisten tarpeiden, aseman ja arvojen turvaamista ja säilyttämistä.

Turvallisuuden käsitteeseen liittyy vahvasti myös turvattomuuden tunne. Turvattomuus nähdään turvallisuuden vastakohtana, jolloin yksilö ei tunne oloansa turvalliseksi. Turvattomuus ilmenee Niemelän (2000) mukaan monenlaisina oireina: pelkoina, psykosomaattisena oirehdintana tai huolestuneisuutena. Yksilön yleisen hyvinvoinnin kannalta onkin tärkeää, että yksilö kokisi olonsa mahdollisimman turvalliseksi.

Terveyden ja hyvinvoinnin laitoksen mukaan Suomessa vuonna 2014 erilaisiin tapaturmiin kuoli lähes 2500 henkilöä. Tapaturmista 89 % tapahtui kotona ja vapaa-ajalla, 10 % tieliikenteessä ja 1 % työpaikoilla. (THL, Tapaturmat Suomessa, 2014). Ryynänen (2000) kirjoittaa artikkelissaan, miten terveysongelmat, sairaudet, väkivalta ja muut vammautumisen uhat aiheuttavat yksilölle pelkoa ja epävarmuutta. Terveydenhuollossa hyödynnetty esineiden internet pystyykin tehostamaan esimerkiksi diagnoosien tekemistä, mikä vähentää vääriä diagnooseja ja helpottaa yksilön pääsyä nopeammin hoitoon. Esineiden internetillä voidaan myös vähentää yksilön mahdollisesti kokemaa väkivaltaa ja vähentää liikenneonnettomuuksia. Tutkielman luvussa 4 esitellään tarkemmin, millä tavoin esineiden internet voi estää muun muassa osan tapaturmista, kuolemista, vammautumisista ja liikenneonnettomuuksista.

3.2 Esineiden internetin turvallisuusongelmat

Vaikka tutkielmassa keskitytään esineiden internetin tuomiin turvallisuushyötyihin, on myös kerrottava monista turvallisuusongelmista ja -riskeistä, joita esineiden internet aiheuttaa. Samalla kun internetiin yhdistyvien esineiden määrä kasvaa esineiden internetin myötä, myös mahdollisuudet niiden heikkouksien hyväksikäyttöön kasvavat. Turvallisuus on merkittävä haaste, koska teknologiaa hyödyntävien esineiden tietoturvan takaamiseksi ei ole olemassa yhteisiä sovittuja käytänteitä. (Al-Fuqaha ym., 2015.)

Mikäli esineiden tietoturva on huonosti toteutettu, esineistä tulee otollisia kohteita erilaisille hyökkäyksille. Esineitä voidaan uudelleenohjelmoida haitallisia tarkoituksia varten tai muuten vahingoittaa hyökkäyksillä. Koska esineiden internetin perustana on toisiinsa kytköksissä olevat esineet, voi yksi saastunut esine saastuttaa useita muita esineitä verkon välityksellä. (Rose ym., 2015.) Esimerkiksi viruksella saastutettu kodin älykäs hälytysjärjestelmä saattaa tartuttaa viruksen myös muihin kodin älykkäisiin esineisiin verkon välityksellä. Mikäli hyökkäyksen avulla hälytysjärjestelmä saadaan epäkuntoon, on koti altis murtovarkaille. Erityisen vaarallisia hyökkäykset ovat esineisiin joiden tarkoitus on auttaa ihmishengen ylläpitämisessä, kuten sydämentahdistimet. Lisäksi koska esineiden internetin avulla yksilöistä kerätään valtava määrä henkilökohtaista tietoa, on tärkeää, etteivät ulkopuoliset henkilöt pääse käsiksi näihin tietoihin. Tietoja ei myöskään saisi pystyä kaappaamaan kesken laitteiden välisen tiedonvälityksen. Yksityisyyden takaaminen onkin turvallisuuden ohella iso haaste, johon esineiden internetin tulee vastata lähivuosina.

Tuwanut ja Kraijak (2015) kirjoittavat, että harvoilla esineiden internetin esineillä on kunnollista tietoturvaa tai muuta sisäistä valvontajärjestelmää hyökkäyksiä vastaan. Ongelmana on, että kunnollinen tietoturva nostaa esineen hintaan, mikä vaikuttaa kuluttajien ostohaluihin ostaa tietoturvallisia esineitä, jos tarjolla on halvempi versio ilman tietoturvaa. Valitettavan moni loppukäyttäjä ei myöskään välitä tai ymmärrä tietoturvan merkitystä eikä näin osaa vaatia sitä laitteelta. Tietoturvavaatimukset tulisikin ottaa huomioon järjestelmäkehityksen elinkaaren jokaisessa vaiheessa, aina tuotteen suunnittelusta valmiin tuotteen ylläpitoon. (Axelrod, 2015.)

Yhtenä vaihtoehtona tietoturvaongelmiin suomalainen tietoturvayhtiö F-Secure on kehittänyt uudenlaisen tietoturvalaitteen SENSE:n. SENSE:n tarkoituksena on suojata kaikkia kodissa olevia älylaitteita viruksia ja hakkereita vastaan. SENSE koostuu älykkäästä reitittimestä, suojaussovelluksesta ja pilvipohjaisesta suojauksesta. (F-Secure 2017.) Tämän tyyppiset ratkaisut suojaavat kodin älykkäitä esineitä kunnes yhdenmukaiset tietoturvaratkaisut saadaan kehitettyä.

4 YKSILÖN TURVALLISUUSHYÖDYT

Tässä luvussa kerrotaan tarkemmin esineiden internetin erilaisista turvallisuushyödyistä yksilölle. Hyötyjä esitellään Atzorin ym. (2010) esittämästä neljästä näkökulmasta, eli yksilön turvallisuushyödyt liikenteessä, terveydenhuollossa, kotona ja henkilökohtaisessa elämässä.

4.1 Turvallisuushyödyt liikenteessä

Nykyisissä ajoneuvoissa on monia erilaisia sensoreita, suorittimia, ohjelmistoja sekä viestintäteknologioita, joiden tarkoituksena on lisätä ajomukavuutta ja ajoturvallisuutta. Wang, Zeng ja Yang (2006) ennustivat artikkelissaan, että lähivuosina ajoneuvojen kyky havainnoida ajoneuvon sisätiloja sekä ajoneuvon ulkoista ympäristöä tulee vakiintumaan ajoneuvoissa. Ajoneuvojen älykkyyden voidaan kyllä sanoa kasvaneen kymmenessä vuodessa erilaisten lisääntyneiden sensoreiden ja järjestelmien, kuten törmäyksenestojärjestelmien, avulla. On kuitenkin todettava, että varsinaiset älyautot ovat vielä kohtalaisen kalliita tavalliselle kuluttajalle. Toisaalta älyautojen, kuten muidenkin älylaitteiden hinta on laskussa teknologian kehittymisen takia ja ehkä jo 10 vuoden päästä älyautot ovat arkipäivää suurelle osalle ihmisistä. Samaan johtopäätökseen on päätynyt Gartner (2015), joka ennustaa lehdistötiedotteessaan, että vuonna 2020 joka viides auto maailmassa olisi yhteydessä internetiin.

Älykkäiden sensorien ja esineiden internetin avulla autoista tehdään entistä älykkäämpiä ja täten lisätään kaikkien tiellä liikkuvien turvallisuutta (Jones, 2002). Esineiden internet mahdollistaa autoille kyvyn havainnoida ja analysoida reaaliajassa erilaisia tiloja ja ympäristöjä. Tällainen tila tai ympäristö voi olla esimerkiksi auton moottoritila, matkustamo tai auton ulkopuolella oleva ympäristö. Älykkäiden sensorien ja viestintäteknologioiden avulla autot pystyvät kommunikoimaan sekä omien laitteidensa, että muiden lähellä olevien autojen kanssa. (Gerla, Lee, Pau & Lee, 2014; Wang ym., 2006.) Erilaisten sensoreiden avulla autot keräävät ja analysoivat tietoa muun muassa kuljettajasta, matkusta-

jista, auton laitteiden toiminnasta, auton ulkopuolella olevasta ympäristöstä sekä tien kunnosta. Myös langattoman sensoriverkon muodostaminen auton sensoreista on mahdollista. (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014)

Auton sisätiloissa olevat sensorit mittaavat auton laitteita ja auton toimintaa, sekä kuljettajan ja matkustajien fyysistä tilaa ja liikettä. Lähes jokaisesta nykyisestä autosta löytyy sensoreita, jotka mittaavat auton toimintaa, kuten moottorin kuntoa tai öljyn määrää. Näiden tavanomaisten sensoreiden lisäksi autoissa voi olla monia muitakin turvallisuutta parantavia sensoreita. Esimerkiksi ratissa ja kuljettajan penkissä olevat sensorit, jotka mittaavat kuljettajan sydämensykettä ja ratin liikkeitä, samalla kun muut autossa olevat sensorit mittaavat kuljettajan pään asentoa, silmien räpytystahtia ja hengitystä (Choi, Han, Kong, & Ko, 2016; Jones, 2002). Yhdistämällä näistä sensoreista saadut tiedot ja analysoimalla niitä auto voi tehdä päätelmiä esimerkiksi kuljettajan väsymyksestä ja varoittaa kuljettajaa nukahtamisvaarasta. Samalla auto voi tällaisessa tilanteessa herättää kuljettajan huomion esimerkiksi avaamalla automaattisesti ikkunan, värisyttämällä kuljettajan penkkiä tai neuvomalla kuljettajaa ajamaan sivuun. (Jones, 2002.) Samalla tavalla auto voi tehdä päätelmiä monesta muustakin turvallisuutta vaarantavasta tilanteesta, kuten sairaskohtaudesta, kuljettajan juopumuksesta tai muusta keskittymisen herpaantumisesta. Älykkäämpiin päätelmiin auto kykenee, mikäli se voi tallentaa sensoreilla keräämäänsä tietoa kuljettajan ajotavoista auton tietokantaan ja vertailla keräämiänsä tietoja (Choi et al., 2016).

Auton eteen ja taakse kiinnitetyt sensorit, tutkat ja kamerat mittaavat auton ympäristöä, tien kuntoa ja ajo-olosuhteita. Näiden sensoreiden, tutkien ja kameroiden tarkoituksena on antaa kuljettajalle tärkeää tietoa auton ympäristöstä ja varoittaa kuljettajaa huonokuntoisesta tiestä tai hankalista ajo-olosuhteista, kuten mustasta jäästä. Internetyhteyden avulla auto puolestaan voi saada hälytyskeskuksesta ajankohtaisen tiedon edessä tapahtuneesta onnettomuudesta ja tarvittaessa ehdottaa vaihtoehtoista reittiä (Jones, 2002). Viestintäteknologioiden avulla auton on myös mahdollista saada tietoa tien kunnosta muilta autoilta. Tällöin auto saisi tietää tarkalleen mistä kohtaa tie on liukas, sillä tämä tieto tulisi autoilta, jotka ovat jo liukkaasta kohdasta ajaneet ja voivat näin välittää reaaliaikaista tietoa eteenpäin. (DXC Technology Company, 2017)

Useimmissa onnettomuustapauksissa kuolinsyy johtuu siitä, ettei oikeanlaista ensiapua ole saatavilla riittävän nopeasti (Chatrapathi, Rajkumar & Venkatesakumar, 2015). Tätä ongelmaa varten autoihin on suunniteltu älykkäitä hälytysjärjestelmiä, joiden avulla apu on nopeammin perillä. Yksi esimerkki tällaisesta hälytysjärjestelmästä on eurooppalainen eCall-järjestelmä, joka on tarkoituksena saada kaikkiin Euroopassa tiellä liikkuviin ajoneuvoihin. Onnettomuuden sattuessa eCall osaa tehdä hälytyksen lähimpään hätäkeskukseen automaattisesti. Puhelun mukana menee tieto ajoneuvon sijainnista, kulkusuunnasta onnettomuushetkellä, ajoneuvotyypistä ja matkustajien lukumäärästä. eCallin etuna on se, että se on yhdenmukainen ja hälytykset kulkeutuvat suoraan eurooppalaiseen hätänumeroon 112, toisin kuin monet muut autovalmistajien omat hälytysjärjestelmät, joissa hälytys kulkeutuu ensin autovalmista-

jien omiin keskuksiin ja sieltä vasta varsinaiseen hälytyskeskukseen. (Häläri, 2016. On mahdollista että kehittämällä eCallia entisestään, se voisi tulevaisuudessa myös lähettää paljon muutakin arvokasta tietoa, kuten sensoreiden keräämät tiedot matkustajilta mitatuista elintoiminnoista tai iskun voimakkuudesta. Tällöin ensiavulla olisi tarkempi tieto siitä, millaisia vammoja onnettomuuspaikalla on odotettavissa.

Atzor ym. (2010) ja Wang ym. (2006) esittävät että ajoneuvojen lisäksi myös teiden infrastruktuuri, eli tiet, jalkakäytävät, liikennevalot ja katulamput olisivat tulossa yhä älykkäämmäksi sensoreiden avulla. Tällöin esimerkiksi vaarallisten aineiden kuljetusta voitaisiin seurata etänä, jolloin kuljetukselle osataan neuvoa turvallisin reitti perille. Katuvalot puolestaan voisivat automaattisesti säätää kirkkauttaan sääolojen, ihmisten läsnäolon tai sen mukaan, mikä aika päivästä on (Zanella et al., 2014).

4.2 Turvallisuushyödyt terveydenhuollossa

Niemelän mukaan ”sairaudet ja taudit ovat keskeisiä turvattomuustekijöitä. Ne aiheuttavat kipua, kärsimystä, toimintakyvyttömyyttä ja kuolemaa.” (Niemelä, 2000, 32). Niemelä (2000) kirjoittaa myös, miten ihmisen toimintakyky on yksi keskeisimmistä turvallisuuden lähteistä, sillä toimintakyvyn avulla ihminen hallitsee ympäristöään ja elämäänsä, mikä luo kokemusta turvallisuudesta. Sairaudet ja vammat puolestaan ovat uhka ihmisen toimintakyvyn säilymiselle ja siten myös yksilön turvallisuudelle, etenkin ikääntyvillä ihmisillä. Ryynäsen mukaan, ”terveyden ja toimintakyvyn ylläpitoon liittyvät kysymykset ja samalla terveysuhkien välttäminen, terveysriskien arviointi ja hallinta ovat tärkeä osa länsimaista terveyspolitiikkaa.” (Ryynänen, 2000, 41-42).

Terveydenhuolto on yksi tärkeimmistä esineiden internetin sovellusalueista, jolla yksilön turvallisuutta voidaan parantaa. Hyödyntämällä puettavaa teknologiaa ja erilaisia sensoreita saadaan terveydenhuollon eri osa-alueista tarkempia, tehokkaampia, luotettavampia ja nopeampia. Tutkielmassa terveydenhuollon osa-alueilla tarkoitetaan diagnosointia, hoidon kartoittamista ja tarjoamista sekä itse hoitoa. (Almotiri, Khan & Alghamdi, 2016). Keskeinen osa terveydenhuoltoa ovat lääkinnälliset laitteet, eli erilaiset instrumentit, laitteistot, välineet, ohjelmistot ja materiaalit joita hyödynnetään ihmisen kokonaisvaltaisessa terveydenhuollossa joko yksinään tai yhdistelmänä (Valvira, 2015). Liittämällä näihin laitteisiin sensoreita ja kyky välittää tietoa esimerkiksi RFID-tunnisteen, Bluetoothin tai Wi-Fin avulla, niistä muodostuu älykkäitä laitteita, joilla voidaan mitata monia arvoja. Mitattavia arvoja voi olla muun muassa verenpaine, sydämensyke, sokeriarvot tai kehon lämpötila. (Almotiri ym., 2016; Sundmaeker ym., 2010.) Tällaisten lääkinnällisten laitteiden mittaamia arvoja voidaan seurata reaaliajassa, mikä mahdollistaa nopean reagoinnin tilanteeseen, mikäli jotain poikkeavaa ilmenee (Almotiri et al., 2016)

Esimerkkinä potilaan sydämentahdistin, joka kerää jatkuvasti tietoja potilaan sydämen toiminnasta. Sydämentahdistin välittää keräämänsä tiedot

Bluetoothin avulla potilaan omaan älypuhelimeen. Älypuhelin voi sen jälkeen analysoida tietoja ja soittaa lääkärille, mikäli tilanne sitä vaatii. (Kopetz, 2011.) Sensoreita voidaan laittaa myös yksilön kotiympäristöön ja arkipäiväisiin eilääkinnällisiin esineisiin, jolloin yksilön terveydentilaa voidaan tarkkailla vieläkin tarkemmin.

Kotiympäristössä olevilla sensoreilla voidaan tarkkailla muun muassa potilaan käyttäytymistä ja lähettää muistutuksia tai ohjeita tarvittaessa television tai radion välityksellä (Zheng & Jamalipour, 2009). Tämä mahdollistaa esimerkiksi dementiapotilaille mahdollisuuden asua omassa kodissaan pidempään ja kotona toipuvien leikkauspotilaiden tarkemman jälkiseurannan. Tilastokeskuksen vuoden 2015 tilaston mukaan Suomessa yleisin kuolemaan johtanut tapaturma aiheutuu kaatumisesta tai putoamisesta. Vuonna 2015 kaatumiset ja putoamiset aiheuttivat noin puolet kaikista tapaturmakuolemista ja kaatumisturmista hieman alle puolet sattui kodissa tai sen välittömässä läheisyydessä. Neljännes kaatumisturmista tapahtui hoitolaitoksissa. (Tilastokeskus, 2015). Sensorit voivatkin lähettää hälytyksen, mikäli potilas kaatuu kotona ja tarvitsee välitöntä apua (Zheng & Jamalipour, 2009).

Esineiden internetiä voidaan terveydenhuollossa hyödyntää myös lääkityksessä. RFID-teknologialla voidaan seurata ja tarkkailla yksittäisiä lääkkeitä ja kokonaisia lääke-eriä, mikä helpottaa väärennettyjen lääkkeiden havaitsemista ja vähentää mahdollisia petoksia toimitusketjuissa (Sundmaeker ym., 2010.) Yksittäisten lääkkeiden kohdalla RFID-teknologiaa voidaan käyttää varmistamaan, että potilaalle annetaan oikeaa lääkettä, oikea annosmäärä ja varmistamaan ettei yksilö ole allerginen jollekin lääkkeen ainesosalle (Akyildiz, Su, Sankarasubramaniam & Cayirci, 2002). Lääkkeessä olevan tunnisteen avulla potilas voi lukea lukulaitteellaan lääkkeen tiedot samalla kun järjestelmä automaattisesti vertaa lääkkeen tietoja potilaan omiin elektronisiin potilastietoihin ja mahdollisiin allergioihin (Islam, Kwak, Kabir, Hossain & Kwak, 2015).

Sairaaloissa esineiden internetiä voidaan käyttää potilaiden, hoitohenkilökunnan, lääkkeiden ja lääkinnällisten laitteiden ja tarvikkeiden seurantaan RFID-tunnisteiden avulla (Atzori ym., 2010). Esimerkiksi lääkinnällisten tarvikkeiden seurannalla voidaan varmistaa, että mikään tarvike ei pääse loppumaan kriittisellä hetkellä tai ettei potilaaseen jää leikkauksen jälkeen vierasesineitä. IBM on hyödyntänyt Ohiolaisessa sairaalassa RFID-teknologiaa ja sensoreita seuraamaan hoitohenkilökunnan käsienpesua jokaisen potilaskontakin jälkeen. Potilashuoneen ovella on sensoreita, jotka havaitsevat kun hoitohenkilökunta liikkuu sisään tai ulos ovesta. RFID-tunnisteet ja muut sensorit pitävät reaaliaikaista kirjaa käsienpesupisteen käytöstä. (IBM, 2013). Käsienpesun parantamisella voidaan estää tulehduksia, jotka aiheuttavat Yhdysvalloissa noin 90 000 ihmisen kuoleman vuosittain (Al-Fuqaha ym., 2015).

Tilanteissa joissa potilas on hengenvaarassa ja tajuton, eikä siten pysty kommunikoimaan hoitohenkilökunnan kanssa, potilaan kehoon kiinnitetty implantti voi pelastaa ihmishenkiä. Implantin avulla potilaan henkilöllisyys on mahdollista tunnistaa ja varmentaa. Lisäksi tunnistamisen yhteydessä potilaan

potilastiedoista saadaan tärkeitä tietoja, jotka vaikuttavat potilaan hoitoon, kuten tieto veriryhmästä ja lääkeallergioista. (Sundmaeker ym., 2010.)

4.3 Turvallisuushyödyt kotona

Sensorit ja toimilaitteet voivat taloissa ja toimistoissa tehdä yksilön elämästä mukavampaa monella tapaa. Ne voivat säätää huoneen lämmityksen mielihalun tai sään mukaan ja huoneen valaistus voi muuttua kellonajan mukaan. Yksilön turvallisuuteen sensorit ja toimilaitteet vaikuttavat kotona pääasiassa tarkkailulla ja hälytysjärjestelmillä. (Atzori ym., 2010.) Rakennuksia voidaan tarkkailla erilaisten vuotojen, tulipalojen, murtojen ja vandalismin varalta (Sundmaeker ym., 2010).

Li ym. (2011) esittävät että tulevaisuudessa asumme kokonaan älykkäissä taloissa, joissa elektronisissa laitteissa ja järjestelmissä olevat sensorit ja toimilaitteet osaavat itse määrittää asetuksensa ja niitä voidaan ohjata etänä internetin välityksellä. Tämä mahdollistaa monenlaisen valvonta- ja hallintakäytön. Lin ja kumppaneiden näkemys on jo suurelta osin toteutunut, sillä kuluttajilla on nykypäivänä mahdollisuus täyttää talonsa erilaisilla älykkäillä laitteilla, joita he voivat ohjata etänä. Esimerkiksi suomalaisella Cozify-yhtiöllä on myynnissä Cozify Hub-kotiautomaatiotuote, jolla käyttäjä voi älypuhelimella internetyhteyden avulla säätää esimerkiksi kodin valaistusta tai lämpötilaa haluamallaan tavalla (Cofizy, 2017). Lin ym. (2011) esittämät älykkään kodin laitteet ja järjestelmät ovat kuitenkin tästä vielä askeleen edempänä, sillä ne havaitsisivat ja tallentaisivat käyttäjän käytöstä automaattisesti, analysoisivat sitä ja ennustaisivat käyttäjän käyttäytymistä analyysinsa perusteella itsenäisesti. Tällaisen älykodin tarkoituksena on tehdä käyttäjän elämästä mukavampaa, tehokkaampaa ja turvallisempaa, sillä älykoti osaisi mukautua käyttäjän vaatimuksiin ilman erillistä ohjausta. (Li ym., 2011.) Nykyisistä kaupallisista laitteista puuttuu vielä suurelta osin tällainen itsenäinen ajattelu. Sundmaekerin ym. (2010) mukaan koneopin kehittymisen ja lisääntyneen käytön myötä yhä useammat esineet yksilön ympäristössä voivat kuitenkin oppia itsenäistä ajattelua, tarkkailla yksilöä ja näin huolehtia yksilöstä. Kodin esineet oppisivat yksilön säännölliset rutiinit ja hälyttäisivät mikäli yksilön rutiineissa havaittaisiin poikkeama. (Sundmaeker ym., 2010.)

Hälytysjärjestelmät ovat tyypillinen esimerkki esineiden internet hyödyntämisestä yksilön turvallisuudessa. Kodali, Jain, Bose & Boppana, 2016 ovat kehittäneet oman prototyyppinsä hälytysjärjestelmästä, jonka tarkoituksena on valvoa luvatonta oleskelua henkilön tontilla. Ideana on, että talon ulkopuolelle on asetettu sensoreita ja kameroita, jotka havainnoivat talon lähistöllä tapahtuvaa liikkumista. Sensoreita on voitu upottaa myös maahan, jolloin niitä voidaan käyttää liikkeen havainnointiin esimerkiksi paineen tai tärinän perusteella (Zheng & Jamalipour, 2009). Mikäli omistajan poissa ollessa nämä sensorit havainnoivat liikettä talon sisäänkäynnin lähellä, ne lähettävät ilmoituksen omistajalle internetin välityksellä. Omistaja voi ilmoituksen avulla käynnistää häly-

tyksen tai hälytys voidaan valinnaisesti lähettää myös suoraan vartiointifirmalle. Toisaalta, jos omistaja huomaa, että taloon saapuva henkilö ei ole tunkeilija vaan tuttu henkilö, omistaja voi hälytyksen sijaan avata oven tulijalle etänä. (Kodali, Jain, Bose & Boppana, 2016.) Tämän tyyppisiä hälytysjärjestelmiä on jo useita markkinoilla ja laajasti käytössä. Sensoreihin perustuvassa kodin tarkkailussa on mahdollista myös hyödyntää langattomia sensoriverkkoja, jolloin tieto liikkuu sensorilta toiselle ja sensorit tekevät yhdessä päätöksiä. Kun ovella oleva sensori havaitsee liikettä ovella, se ilmoittaa havainnosta toiselle sensorille, joka puolestaan kytkee valvontakameran ja äänentallennuksen päälle. Saman aikaisesti kaikki sensorit keräävät tietoa ympäristöstään ja välittävät tietonsa käyttäjälle. (Hong, Yang & Rong, 2016).

Toinen yleinen tapa jolla esineiden internet suojaa kotia on erilaisten vaarojen havainnointi kodin sisällä sensoreiden avulla ja vaaroista varoittaminen toimilaitteella. Tyypillinen esimerkki tällaisesta on palovaroitin. Kun sensorit havaitsevat mahdollisen tulipalon (esimerkiksi lämpötilasensoreilla), ne lähettävät ilmoituksen toimilaitteelle, joka varoittaa asunnossa olijoita. Lisäksi älykäs palovaroitin lähettää hälytyksen automaattisesti myös suoraan hätäkeskukseen. Hälytyksen yhteydessä voidaan lähettää muitakin sensorien keräämiä tietoja, kuten tieto palavasta materiaalista, palon laajuudesta ja ihmisten läsnäolosta asunnossa. (Miorandi, Sicari, De Pellegrini & Chlamtac, 2012.)

4.4 Yksilön henkilökohtaiset turvallisuushyödyt

Esineiden internetiä voidaan hyödyntää auttamaan yksilöä saamaan nopeammin apua, mikäli tämä joutuu väkivallan kohteeksi. Alisha, Jatti, Kannan, Vijayalakshmi ja Sinha (2016) ovat suunnitelleet puettavaa älykästä laitetta, joka turvaisi intialaisia naisia ja tyttöjä väkivallalta, erityisesti raiskauksilta. Intiassa raiskaus on neljänneksi yleisin naisiin kohdistuva rikos. Alishan ym. (2016) suunnittelema laite mittaisi tauotta käyttäjän fyysisiä arvoja, kuten hikoilun määrää, kehon lämpötilaa ja kehon asentoa. Kerätty data analysoidaan ja mikäli datan perusteella käyttäjä vaikuttaa olevan vaarassa, laite lähettää hälytyksen määritetylle taholle. Erilaisia turvahälyttimiä on jo olemassa, mutta ne tarvitsevat ihmisen aktivoimaan hälytyksen, esimerkiksi nappia painamalla. Alishan ym. (2016) mukaan uhkaavassa tilanteessa laite, joka vaatii erillisen käyttäjän tekemän hälytyksen, ei ole ideaalista, joten heidän suunnittelemansa malli toimisi täysin automaattisesti.

Teknologian tutkimuskeskus VTT puolestaan on kehitellyt myös puettavaa teknologiaa älyvaatteiden muodossa. VTT:n kehittelemien älyvaatteiden tarkoituksena on kerätä tietoa käyttäjästä ja ympäristöstä ja tehdä näiden tietojen perusteella päätelmiä siitä tarvitseeko käyttäjää kenties lämmittää tai viilentää. Älyvaate osaisi analyysinsa perusteella pitää käyttäjän lämpökokemuksen aina optimaalisena. (VTT, 2016). Erityisen hyödyllistä turvallisuuden kannalta tämä olisi vauvoille, jotka eivät itse osaa vähentää tai lisätä vaatetusta, sekä

henkilöille, jotka työskentelevät vaativissa olosuhteissa hyvin kuumassa tai hyvin kylmässä.

Esineiden internetiä voidaan hyödyntää varkaustilanteiden havaitseminen ja tärkeiden esineiden seurantaan. RFID-teknologian avulla voitaisiin seurata, että haluttuja laitteita ei siirretä rajatulta alueelta ilman lupaa. Tällaisia esineitä voisi olla esimerkiksi tietokone, kalliit koriste-esineet tai arvokkaat korut. Mikäli esine poistuu ilman annettua valtuutusta rajatulta alueelta, kuten talosta tai toimistosta, käyttäjälle ja halutessa vartiointifirmalle lähtee automaattisesti hälytys ryöstöyrityksestä. (Atzori ym., 2010.) Tieto siitä että tärkeitä esineitä ei voida siirtää merkityltä alueelta ilman että yksilö saa tiedon asiasta luo turvallisuuden tunnetta.

Turvallisuushyötyjä saadaan myös lasten liikkumisen seurannalla. Suomessa tehdyssä kenttätutkimuksessa 16 ala-asteella olevalle oppilaalle annettiin GPS-paikannin ja RFID-tunniste. GPS-paikannin seurasi lapsen liikkumista ulkona ja RFID-tunniste koulun sisällä. Koulun sisällä olevat RFID-lukijat havaitsivat ja tallensivat tiedon kun oppilas tuli tai lähti koulusta. Vanhemmat pystyivät seuraamaan reaaliajassa, missä lapsi milloinkin oli ja missä lapsi on liikkunut. Opettajat puolestaan näkivät oliko lapsi tullut kouluun vai ei. (Ervasti, Laitakari, & Hillukkala, 2016) Pienillä yksin liikkuvilla lapsilla tällainen seurantakeino varmasti tukee aikuisen turvallisuuden tunnetta, kun vanhempi tietää aina tarkalleen missä lapsi on.

5 YHTEENVETO

Tutkielmassa käytiin läpi esineiden internetin hyötyjä yksilölle turvallisuuden näkökulmasta. Turvallisuushyödyt esiteltiin neljän käyttökohteen kautta, jotka olivat liikenne, terveydenhuolto, koti ja yksilön henkilökohtainen elämä. Turvallisuushyötyjen esittelyn lisäksi kerrottiin myös esimerkkien avulla, millä tavoin esitetyt hyödyt konkreettisesti lisäävät yksilön turvallisuutta ja turvallisuuden tunnetta.

Tutkielmassa esiteltiin useita hyötyjä, joita yksilö voi jo nyt hyödyntää turvallisuutensa lisäämisessä, kuten kodin hälytysjärjestelmät, tai jotka ovat mahdollisesti tulossa lähitulevaisuudessa laajemmin käyttöön, kuten potilaiden tunnistaminen. Terveydenhuolto ja älykäs liikenne osoittautuivat tutkielmassa monipuolisimmiksi alueiksi turvallisuuden lisäämisessä. Se ei ole yllättävää, sillä varsinkin terveydenhuolto on isossa osassa ihmisten elämää ja terveydenhuollon kehittämisellä kehitetään koko yhteiskuntaa. Yksilön henkilökohtaiset turvallisuushyödyt jäivät muita suppeammaksi. Tämä johtui osittain siitä, että rajanveto eri käyttökohteiden välillä ei aina ollut selvää. Esimerkiksi yksilön henkilökohtaisen terveydentilan seuranta voidaan laskea sekä terveydenhuollon turvallisuushyödyksi, että yksilön henkilökohtaiseksi turvallisuushyödyksi.

Tutkielmassa selvisi että esineiden internetin tärkeimmät hyödyt voidaan jakaa ominaisuuksiensa perusteella neljään osa-alueeseen:

- Tietojen kerääminen
- Kerätyn tiedon analysointi
- Esineiden välinen tiedonvälitys
- Esineiden ja yksilön välinen tiedonvälitys

Esineiden internetin keräämä tieto yksilöstä mahdollistaa yksilölle entistä tarkemman kuvan omasta tilasta ja yleisesti yksilön ympäristöstä. Esimerkiksi terveydenhuollossa tietojen kerääminen, kuten terveydentilan seuranta sensorien avulla, nopeuttaa oikean diagnoosin tekemistä, sillä lääkärillä on käytössään valtava määrä sensorien keräämää tietoa, josta voidaan louhia diagnoosin kannalta keskeisimmät tiedot. Kerätyn tiedon analysointi puolestaan mahdollistaa

esimerkiksi nopeamman ensiavun saamisen onnettomuuspaikalle. Oli sitten kyseessä vakava kaatuminen kotona, autolla ajettu onnettomuus tai tulipalo, kerätyn tiedon perusteella esineet osaavat analysoida tilannetta ja tarvittaessa toimia analyysinsa mukaan. Esineet voivat esimerkiksi hälyttää tarvittaessa apua onnettomuuspaikalle ilman ihmisen erillistä käskyä. Tärkeää on myös esineiden keskeinen tiedonvälitys, jolla mahdollistetaan esimerkiksi juurikin hälytyksen lähettäminen hätäkeskukselle, kun sensorit ovat ensin analysoineet hälytyksen tarpeen keräämänsä tiedon perusteella. Esineiden ja yksilön välinen tiedonvälitys on neljäs tärkeä osa-alue. Esineet voivat varoittaa yksilöä esimerkiksi tulipalon vaarasta tai kertoa tärkeää tietoa ajo-olosuhteista. Esineiden internet toimiikin parhaiten ja mahdollistaa parhaan hyödyn, kun jokaista kategorian osaa käytetään yhdessä. Taulukkoon 1 on vielä koottu taulukkomuodossa keskeisiä havaintoja yksilön turvallisuushyödyistä. Kaikki tutkielmassa esitellyt turvallisuushyödyt yhdessä vähentävät tapaturmia ja sitä kautta estävät kuolemia ja vammautumisia.

Taulukko 1 Kooste esineiden internetin hyödyntämisestä yksilön turvallisuudessa

	Tietojen kerääminen	**Kerätyn tiedon analysointi**	**Esineiden välinen tiedonvälitys**	**Esineiden ja yksilön välinen tiedonvälitys**
Miten	Sensorit, RFID-tunnisteet	Internet, laitteen omat mikroprosessorit	Langattomat sensoriverkot, Bluetooth, Wi-Fi, matkapuhelinverkot	Toimilaitteet, internet, Bluetooth, Wi-Fi, matkapuhelinverkot
Esimerkkejä käyttötilanteista	Auton toiminnan seuranta, terveydentilan seuranta, ympäristön tarkkailu, lapsen paikkatietojen seuranta	Kaatuminen kotona, poikkeava terveydentila, potilaan tunnistaminen	Luvaton liikkuminen alueella, käsienpesun laiminlyönti, tieto hätäkeskukselle onnettomuudesta	Tieto ajo-olosuhteista, varoitukset (väsynyt kuski, tulipalo, murtautuminen)

Esineiden internetin ongelmana on sen huono tietoturva. Yhtenä syynä on että yhteiset käytänteet kaikkien valmistajien kesken puuttuvat ja jokainen valmistaja toteuttaa laitteen tietoturvan näkemällään tavalla. Lisäksi yksityisyyden suojaaminen puutteellista ja yksilöllä ei useinkaan ole tietoa siitä, ketkä kaikki hänen tietojansa pääsee lukemaan tai muokkaamaan. Tämän johdosta esineiden internetin laajamittaista hyödyntämistä on vielä harkittava tarkkaan, eikä hyötyjä tule tällaisenaan ottaa sokeasti käyttöön ennen kuin tietoturva- ja yksityi-

syysongelmat on saatu käsiteltyä. Ajatuksena monet turvallisuushyödyistä kuulostavat hyvältä, kuten teknologia, joka automaattisesti pitää kirjaa talossa olevista henkilöistä ja talon ulkopuolella tapahtuvasta liikkeestä ja hälyttää tarvittaessa vartiointifirmalle. Tällaiseen hälytysjärjestelmään on kuitenkin hankala luottaa täydellisesti, mikäli järjestelmässä esiintyy tietoturvaheikkouksia ja on mahdollista, että järjestelmä voidaan sammuttaa etänä käyttäjän huomaamatta. Puhumattakaan implanteista tai elintoimintoja ylläpitävistä esineistä, kuten sydämentahdistimesta. Näiden esineiden kanssa yksilön on oltava vieläkin tarkempi, että tietoturva on kunnossa. Tietoturvaongelmia voi kuitenkin vähentää esimerkiksi älykkäällä koko kodin suojaamiseen tarkoitetulla tietoturvajärjestelmällä.

Esineiden internetin vallankumous on kuitenkin jo alkanut ja lopputuloksena voi todeta että tietoturvaongelmista huolimatta, esineiden internet tarjoaa paljon turvallisuushyötyjä, ja sen järkevällä hyödyntämisellä on valtava potentiaali yksilön turvallisuuden lisäämisessä.

LÄHTEET

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer Networks*, *38*(4), 393–422.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376.

Alisha, R. M., Vijayalakshmi, P., Jatti, A., Kannan, M. & Sinha, S. (2016). Design and Development of an IOT based wearable device for the Safety and Security of women and girl children. In *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016 - Proceedings* (pp. 1108–1112).

Almotiri, S. H., Khan, M. A. & Alghamdi, M. A. (2016). Mobile Health (m-Health) System in the Context of IoT. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 39–42.

Atzori, L., Iera, A. & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Axelrod, C. W. (2015). Enforcing security, safety and privacy for the Internet of Things. *2015 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2015*, (January), 1–6.

Buckley, J. (2006). From RFID to the Internet of Things: Pervasive networked systems. *Proceedings of the Pervasive Networked Systems Conference*, (March), 32.

Chatrapathi, C., Newlin Rajkumar, M. & Venkatesakumar, V. (2015). VANET based integrated framework for smart accident management system. *Proceedings of the IEEE International Conference on Soft-Computing and Network Security, ICSNS 2015*.

Choi, Y., Han, S. I., Kong, S. & Ko, H. (2016). Driver Status Monitoring Systems for Smart Vehicles Using Physiological Sensors. *EEE Signal Processing Magazine*, *33*(6), 22–34.

Cofizy. 2017. Haettu 20.6. osoitteesta https://www.cozify.fi/

Coetzee, L. & Eksteen, J. (2011). The Internet of Things - promise for the future? An introduction. *IST-Africa Conference Proceedings, 2011*, 1–9.

Collin, J., & Saarelainen, A. (2016). *Teollinen internet* (1. painos). Talentum.

DXC Technology Company. (2017). *The Internet of Things and Connected Cars with IoT on Board*.

Ervasti, M., Laitakari, J. & Hillukkala, M. (2016). "I want to know where my child is at all times" – field study of a location-aware safety service for schoolchildren. *Behaviour & Information Technology*, *35*(10), 833–852.

F-Secure (2017). F-Secure Sense. Haettu 17.6.2017 osoitteesta
https://www.f-secure.com/en/web/home_global/sense

Gartner. (2.2.2017). Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. Haettu 21.6.2017 osoitteesta http://www.gartner.com/newsroom/id/3598917

Gartner. (26.1.2015). Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities. Haettu 11.6.2017 osoitteesta:
http://www.gartner.com/newsroom/id/2970017

Gerla, M., Lee, E.-K., Pau, G. & Lee, U. (2014). N/A - Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 241–246.

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Gupta, R. & Gupta, R. (2016). ABC of Internet of Things: Advancements, benefits, challenges, enablers and facilities of IoT. *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*.

Hong, X., Yang, C. & Rong, C. (2016). Smart Home Security Monitor System. *2016 15th International Symposium on Parallel and Distributed Computing (ISPDC)*, 247–251.

Häläri. (4.10.2016). Auto, joka soittaa hätäpuhelutkin itse. Haettu 10.6.2017 osoitteesta http://www.112.fi/halari/uusiteknologia/teknologia/10/0/auto_joka_soittaa_hatapuhelutkin_itse_70105

IBM Research. (18.11.2013). Sensors remind doctors to wash up. Haettu 19.6.2017 osoitteesta https://www.ibm.com/blogs/research/2013/11/sensors-remind-doctors-to-wash-up/

Internet Live Stats. Internet Users. Haettu 27.5.2017 osoitteesta
http://www.internetlivestats.com/internet-users/

Islam, S. M. R., Kwak, D., Kabir, H., Hossain, M. & Kwak, K.-S. (2015). The Internet of Things for Health Care : A Comprehensive Survey. *IEEE Access*, *3*, 678–708.

Jia, X., Feng, Q., Fan, T. & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 1282–1285.

Jones, W. D. (2002). Building safer cars. *IEEE Spectrum*, *39*(1), 82–85.

Juels, A. (2006). RFID Security and Privacy : A Research Survey. *IEEE Journal on Selected Areas in Communications*, *24*(2), 381–394.

Jurvansuu, M., & Belloni, K. (2013). *Productivity leap with ioT. Visions of the Internet of Things with a special focus on Global Asset Management and Smart Lighting*. VTT Technical Research Centre of Finland.

Kodali, R. K., Jain, V., Bose, S. & Boppana, L. (2016). IoT Based Smart Security and Home Automation System, 1286–1289.

Kopetz, H. (2011). Internet of Things. In *Real-Time Systems* (pp. 307–323). Springer US.

Kortuem, G., Kawsar, F., Fitton, D. & Sundramoorthy, V. (2010). Smart objects as building blocks for the Internet of things. *Internet Computing, IEEE*, *14*(1), 44–51.

Li, X., Lu, R., Liang, X., Shen, X., Chen, J. & Lin, X. (2011). Smart community: An internet of things application. *IEEE Communications Magazine*, *49*(11), 68–75.

Maslow, A. H., & Frager, R. (1987). *Motivation and personality* (3rd ed.). New York: Harper and Row.

Miorandi, D., Sicari, S., De Pellegrini, F. & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516.

Niemelä, P. & Lahikainen, A. R. (2000). *Inhimillinen turvallisuus*. Tampere: Vastapaino.

Puolustusministeriö. (2007). *Puolustusministeriön turvallisuustoiminnan strategia*. Kirjapaino Keili Oy.

Rose, K., Eldridge, S. & Chapin, L. (2015). THE INTERNET OF THINGS: AN OVERVIEW. Understanding the Issues and Challenges of a More Connected World. *The Internet Society*, (October), 80.

Ryynänen, U. (2000). *Terveys ja turvallisuus*. Teoksessa Niemelä, Pauli
& Lahikainen, Anja-Riitta: Inhimillinen turvallisuus. Vastapaino, Tallinna.

Sipponen, K. (1990). *Yhteisön turvallisuus kansalaisen turvallisuuden ehtona*. Teoksessa Oikeus turvallisuuteen. Perusturvallisuuden elementtien tarkastelua. Turku: [Turvallisuustieteellinen tutkimuskeskus].

SPEK (2014). *Kokonaisturvallisuuden sanasto*. Sanastokeskus TSK ry & Suomen Pelastus- alan Keskusjärjestö SPEK.

Sundmaeker, H., Guillemin, P., Friess, P. & Woelfflé, S. (2010). *Vision and challenges for realizing the internet of things*. *European Commission*.

Swan, M. (2012). Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, *1*(3), 217–253.

Tilastokeskus (2016). Kaatuminen yleisin tapaturmakuoleman syy. Haettu 24.5.2017 osoitteesta https://www.tilastokeskus.fi/til/ksyyt/2015/ksyyt_2015_2016-12-30_kat_005_fi.html

Tozlu, S., Senel, M., Mao, W. & Keshavarzian, A. (2012). Wi-Fi enabled sensors for internet of things: A practical approach. *IEEE Communications Magazine*, *50*(6), 134–143.

Tuwanut, P. & Kraijak, S. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, 6 .-6 .

Valvira (2015). Terveydenhuollon laitteet ja tarvikkeet. Haettu 23.5.2017 osoitteesta http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet

VTT. (7.3.2016). Haettu 21.6. osoitteesta:
http://www.vtt.fi/medialle/uutiset/vtt-tulevaisuuden-%C3%A4lyvaatetus-s%C3%A4%C3%A4tyy-henkil%C3%B6n-todellisen-tarpeen-mukaan-automaattisesti

Wang, F. Y., Zeng, D. & Yang, L. (2006). Smart cars on smart roads: An IEEE intelligent transportation systems society update. *IEEE Pervasive Computing*, *5*(4), 68–69.

Want, R. (2004). The Magic of RFID. *ACM Queue*, (7), 40–48.

Want, R. (2006). An Introduction to RFID Technology. *IEEE Pervasive Computing*, *5*(1), 25–33.

Whitmore, A., Agarwal, A. & Da Xu, L. (2015). The Internet of Things???A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274.

Xia, F., Yang, L. T., Wang, L. & Vinel, A. (2012). Internet of Things. *International Journal of Communications Systems*, *25*(9), 1101–1102.

Yick, J., Mukherjee, B. & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, *52*(12), 2292–2330.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, *1*(1), 22–32.

Zheng, J., & Jamalipour, A. (2009). *WIRELESS SENSOR NETWORKS A Networking Perspective*. John Wiley & Sons.