Juho Kallioniemi

ESINEIDEN INTERNETIN TURVALLISUUS KULUTTAJAPERSPEKTIIVISTÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Kallioniemi, Juho
Esineiden Internetin turvallisuus kuluttajaperspektiivistä
Jyväskylä: Jyväskylän yliopisto, 2018, 38 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Luoma, Eetu; Palonen, Teija

Esineiden Internetin sovellukset nähdään tulevaisuudessa läsnä kaikkialla ympäristössämme, helpottaen ihmisten arkea ja työtä. Ennen kuin kuluttajat voivat hyväksyä tällaisen jokaiseen elämänalueeseen ulottuvan teknologian, tulee valmistajien ansaita heidän luottamuksensa teknologian turvallisuuteen. Turvallisuus on kuitenkin jäänyt kehityksessä sivurooliin, vaikka esineiden Internetin riskit kuluttajien turvallisuudelle ja yksityisyydelle ovat huomattavia. Tässä kirjallisuuskatsauksena toteutettavassa tutkielmassa esineiden Internetin kyberturvallisuutta lähestytään kuluttajiin kohdistuvien turvallisuusuhkien ja niiden estämiseen tähtäävien keinojen näkökulmasta. Tutkimuskirjallisuudesta tunnistettiin useita konkreettisia uhkia monenlaisten kyberhyökkäysten muodossa. Näihin lukeutuivat muun muassa palvelunestohyökkäykset, datainjektio sekä salauksen murtamiseen tähtäävät hyökkäykset. Suuri osa esineiden Internetin turvallisuusratkaisuista oli kuitenkin esitetty tavoitteina ja konkreettisiakaan keinoja ei yleensä oltu suunniteltu erityisesti esineiden Internetiä varten. Luottamus oli eräs kiinnostavimmista turvallisuuden parantamiseen tähtäävistä keinoista.

Asiasanat: esineiden Internet, kyberturvallisuus, yksityisyys, luottamus

ABSTRACT

Kallioniemi, Juho
Security of the Internet of Things from a consumer perspective
Jyväskylä: University of Jyväskylä, 2018, 38 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Luoma, Eetu; Palonen, Teija

The Internet of Things applications are viewed as ubiquitous technologies in our environment in the future. Consumers' trust in the IoT security should be earner by the manufacturers before they can accept such a pervasive technology in their daily lives. However, security in the development has been severely lacking even though the risks for consumers' security and privacy are substantial. In this literature review, the cybersecurity of the Internet of Things is approached from the perspective of security threats that affect consumers and the proposed solutions for enhancing the IoT security. Multiple concrete threats, mostly in the form of cyberattacks, were identified in the research literature. These include but are not limited to denial of service attacks, false data injection and cryptanalysis. A large portion of the solutions were presented as objectives and even the concrete methods were often not designed for use in the Internet of Things specifically. One of the most interesting solutions was trust.

Keywords: Internet of Things, cybersecurity, privacy, trust

KUVIOT

SISÄLLYS

1 JOHDANTO

Esineiden Internet eli englanniksi Internet of Things (IoT) on yksi ICT-alan merkittävimmistä kasvavista trendeistä, joka nähdään Internetin seuraavana suurena kehitysaskeleena (Miorandi, Sicari, De Pellegrini & Chlamtac, 2012). Miorandi ym. (2012) sanovat esineiden Internetin olevan sateenvarjotermi, jolla tarkoitetaan monenlaisia aspekteja Internetin ja verkon ulottumisesta fyysiseen maailmaan yksilöityjen sensori- tai aktuaattoritoimintoja suorittavien laitteiden välityksellä. Sensoritoiminnoilla tarkoitetaan fyysisen maailman aistimista ja aktuaattoritoiminnoilla toimintojen suorittamista laitteissa, kuten esimerkiksi ikkunan avaus. Internetin tulo osaksi fyysistä maailmaa aiheuttaa muutoksen sen luonteessa tulevan vuosikymmenen aikana, muuttuen saumattomaksi yhdistelmäksi tavanomaisia tietoverkkoja ja toisiinsa kytkeytyneitä älykkäitä laitteita eli "esineitä" (Miorandi ym., 2012). Nämä esineet käsittävät perinteisten tietoteknisten laitteiden, kuten älypuhelinten lisäksi myös kaikenlaiset arkipäiväiset tavarat ja objektit (Gubbi, Buyya, Marusic & Palaniswami, 2013). Tällaisia älykkäitä objekteja voivat olla esimerkiksi kodinkoneet, elintarvikepakkaukset, tiet ym. infrastruktuuri, kulkuneuvot ja terveydenhuollon laitteet (Atzori, Iera & Morabito, 2010).

Lähitulevaisuudessa jokainen esine voidaan yhdistää Internetiin ja niiden määrä on paljon suurempi kuin niitä käyttävien ihmisten (Tan & Wang, 2010). Yhdistettyjen laitteiden määrä ylittikin maailman populaation vuonna 2011 ja vuonna 2020 niitä ennustetaan olevan 24 miljardia (Gubbi ym., 2013) tai jopa 50 miljardia (Covington & Carskadden, 2013). Esineiden sensorit ja aktuaattorit ovat tulevaisuudessa kaikkialla läsnä eli ubiikkeja ympäristössämme. Tiedon jakaminen laitteiden välillä mahdollistaa niiden yhteistoiminnan ja yhteisten päämäärien ja tilannekuvan saavuttamisen. (Gubbi, ym., 2012; Atzori ym., 2010.)

Käyttökohteita esineiden Internetiä hyödyntävälle massiiviselle älykkäiden esineiden verkolle on valtavasti, joista vasta pieni osa on saavutettavissamme (Atzori ym., 2010). Esimerkkejä lähitulevaisuudessa mahdollisista käyttökohteista ovat älykkäästi hallittava liikenne ja logistiikka, potilaiden terveydentilan valvonta sekä älykoti (Atzori ym., 2010).

Turvallisuus on kuitenkin aina merkittävä huolenaihe, kun tietoverkkoja otetaan käyttöön suuressa mittakaavassa (Gubbi ym., 2013). Sicarin, Rizzardin, Griecon ja Coen-Porisinin (2015) mukaan turvallisuuteen liittyy datan eheys, luottamuksellisuus ja anonyymiys sekä autentikoinnin ja valtuutusten varmistaminen. Esineiden Internetin käyttäjiin kohdistuvia turvallisuusuhkia ovat Atamlin ja Martinin (2014) mukaan esimerkiksi laitteiden peukalointi, väärän datan injektointi ja tietovuodot. Esineiden Internet kasvattaa myös Internetin hyökkäyspintaa huomattavasti ja muuttaa kyberhyökkäysten luonnetta (Covington & Carskadden, 2013).

Esineiden Internetin käyttäjiin kohdistuvia riskejä ovat Sicarin ym. (2015) mukaan muun muassa luottamuksellisten tietojen päätyminen vääriin käsiin ja palvelun käyttämättömissä oleminen palvelunestohyökkäyksen takia. He mainitsevat myös fyysiset riskit esimerkiksi auton jarrujen toimimattomuuden takia. Esineiden Internetin turvallisuus liittyy siten perinteisen tietoturvallisuuden sijaan laajemmin kyberturvallisuuteen. Tässä tutkielmassa turvallisuus tarkoittaakin nimenomaan kyberturvallisuutta.

Esineiden Internet on erityisen haavoittuvainen laitteiden rajoitusten takia (Porras, Pänkäläinen, Knutas & Khakurel, 2018; Atamli & Martin, 2014; Sicari ym., 2015; Atzori ym., 2010). Laitteilla on rajallisesti suorituskykyä, muistia ja akkuvirtaa, mikä rajoittaa monimutkaisten ja suorituskykyä vaativien turvallisuustoimintojen käyttöä (Porras ym., 2018). Ongelmia aiheuttaa myös laitteiden jättäminen vartioimattomiksi, mikä helpottaa niihin kajoamista. Kommunikaation langattomuus helpottaa yhteyksien salakuuntelua. (Atzori ym., 2010.) Sicarin ym. (2015) mukaan myös skaalautuvuus on esteenä perinteisten turvatoimien käytössä. Lisäksi haastetta tuottaa verkon epäyhtenäisyys eli heterogeenisyys (Porras ym., 2018; Covington & Carskadden, 2013; Sicari ym., 2015; Atamli & Martin, 2014). Porras ym. (2018) toteavat myös, että olemassa olevien kuluttajille tarkoitettujen IoT-laitteiden ohjelmistotason suojaukset ovat riittämättömiä kokonaisten ympäristöjen turvallisuuden varmistamiseen.

Atamli ja Martin (2014) väittävät, ettei esineiden Internetin arvoa ole mahdollista aliarvioida. Miorandin ym. (2012) mukaan esineiden Internet tarjoaa suunnattomasti liiketoimintamahdollisuuksia yrityksille, jotka luovat älykkäiden esineiden verkkoa ja kehittävät sille sovelluksia. Heidän mukaansa kuluttajat hyötyvät tästä saamalla käyttöönsä paljon uusia aina käytettävissä olevia palveluita tarpeisiinsa.

Porraksen ym. (2018) mukaan IoT-teknologian aikaisten käyttöönottajien keskuudessa on kuitenkin syntynyt epävarmuutta nimenomaan turvallisuuteen liittyen. Myös muut tutkijat puhuvat käyttäjien hyväksynnän ja luottamuksen saamisesta yhtenä tärkeimmistä vaatimuksista esineiden Internetin laajalle käyttöönotolle. Miorandi ym. (2012) peräänkuuluttavat luottamuksellisuuden, todennuksen ja yksityisyyden takaamista järjestelmätasolla, jotta sidosryhmät olisivat halukkaampia IoT-ratkaisujen käyttöönottoon. Kuitenkaan tutkimuksessa ei ole keskitytty laitteiden turvallisuuteen kokonaisen järjestelmän osana vaan lähinnä itsenäisinä kokonaisuuksina (Atamli & Martin, 2014). Sicarin ym. (2015) mielestä käyttäjien luottamuksen saavuttamiseksi tulisi määritellä päte-

vät turvallisuus-, yksityisyys- ja luottamusmallit. Atzorin ym. (2010) mukaan ihmiset vastustavat esineiden Internetiä niin kauan, kunnes yleistä varmuutta siitä, että se ei uhkaa heidän yksityisyyttään, ei ole. Esimerkiksi viimeaikaisessa tutkimuksessa Liu & Zhang (2017) tutkivat Twitter-käyttäjien mielikuvia esineiden Internetistä ja huomasivat, että käyttäjät ovat kyllä kiinnostuneita esineiden Internetistä, mutta ovat erityisesti huolissaan turvallisuudesta ja yksityisyydestä.

Koen edellä mainittujen syiden takia oleellisena kuluttajiin kohdistuvien turvallisuusuhkien ja niiden torjuntaan liittyvien toimien tunnistamisen. Tämä auttaisi esineiden Internetin tuotteisiin ja palveluihin suuntautuvia yrityksiä suojaamaan asiakkaidensa turvallisuuden uskottavasti. Turvallisuusuhkiin on mielestäni syytä varautua IoT-teknologian vasta tehdessä tuloaan, jotta vältyttäisiin uhkakuvien toteutumiselta jo aikaisessa vaiheessa. Koska IoT-teknologiaan sisältyy huomattavasti liiketoimintamahdollisuuksia ja sen turvallisuus käsitetään erityisen haasteelliseksi, uskon, että myöskin kyberturvayrityksillä on potentiaalia tehdä huomattavasti voittoa esineiden Internetin turvallisuusratkaisuilla.

Tämän tutkielman tavoitteena on tunnistaa kirjallisuudesta keskeisimmät esineiden Internetissä kuluttajiin kohdistuvat turvallisuusuhat ja esitetyt keinot niiden torjumiseksi. Turvallisuusuhkia ja niiden torjuntaa käsiteltiin ensisijaisesti olemassa olevan teknologian kontekstissa. Pääasiallinen tutkimuskysymys tutkielmassa oli: miten esineiden Internetin turvallisuutta voidaan parantaa? Apukysymykset liittyivät esineiden Internetin ja sen turvallisuuden ymmärtämiseen. Näistä tärkeimmät olivat: miten esineiden Internet rakentuu ja mitä uhkia kuluttajiin kohdistuu?

Tutkielma toteutettiin kirjallisuuskatsauksena ja sen toteutuksessa sovellettiin Okolin ja Schabramin (2010) ohjetta tietojärjestelmätieteen kirjallisuuskatsauksen tekemiseen. Tiedonhaussa käytiin läpi suuria koottuja tietokantoja ja hakukoneita, tärkeimpinä Google Scholar ja Scopus. Lisäksi käytettiin AIS Electronic Libraryä (AISeL), joka sisältää tietojärjestelmätieteen tutkimuskirjallisuutta. Hakulauseet muodostuivat pääasiassa tutkielman aiheen ”Internet of Things” ja erilaisten hakusanojen yhdistelmistä. Tärkeimpiä hakusanoja olivat “security”, “privacy”, “threats”, “trust” ja “applications”.

Käytännön seulassa kirjallisuuden oli täytettävä tiettyjä praktisia vaatimuksia päästäkseen mukaan tutkimukseen. Kirjallisuuden tuli oltava kirjoitettu joko englanniksi tai suomeksi. Kirjallisuuden oli lisäksi käsiteltävä joko esineiden Internetiä yleisesti tai keskittynyt siihen turvallisuusnäkökulmasta. Vain yritys- tai organisaationäkökulmiin keskittynyt tutkimus hylättiin. Myös selvästi vanhentuneet tutkimukset eliminoitiin.

Seulan läpäisseen kirjallisuuden laatu arvioitiin tutkielman laadun varmistamiseksi. Lähteiksi pyrittiin valitsemaan ensisijaisesti tutkimuksia, joihin oli viitattu eniten. Lähdeviittausten määrää ei kuitenkaan katsottu, jos kyseessä oli erityisen tuore tutkimus. Laadunarvioinnissa pyrittiin sisällyttämään arvostetuimmissa alan julkaisuissa ja konferensseissa julkaistut tutkimukset sekä tutkielman kannalta erityisen relevantit tutkimukset.

Tutkielmassa on kaksi sisältölukua. Ensimmäisessä luvussa esitellään esineiden Internet yleisesti ja tarkastellaan sen tutkielman kannalta oleellisia käyttötapoja. Lisäksi selvitetään esineiden Internetin toteuttamisessa käytettävä teknologia ja arkkitehtuuri ja toteutuksen haasteet. Toisessa sisältöluvussa pureudutaan turvallisuuteen eli määritellään kyberturvallisuus esineiden Internetin kontekstissa, tunnistetaan kirjallisuudesta kuluttajiin kohdistuvia turvallisuusuhkia ja esitetään tapoja parantaa esineiden Internetin turvallisuutta.

2 ESINEIDEN INTERNET

Tässä luvussa esineiden Internet määritellään tutkimuskirjallisuuteen perustuen. Määritelmää jatketaan visioimalla sen oleellisia piirteitä esineiden Internetin luonteen ja toiminnan havainnollistamiseksi. Tämän jälkeen esitellään esineiden Internetin toteutus tarkemmin tarkastellen ensin sen arkkitehtuuria ja sitten relevantteja teknologioita. Arkkitehtuurista esitellään tarkemmin viisikerroksinen malli. Esineiden Internetin sovelluksia tarkastellaan kolmella kuluttajakeskeisellä osa-alueella: älykoti, älykaupunki ja terveydenhuolto. Viimeisessä alaluvussa käydään vielä läpi joitakin esineiden Internetin toteutuksen haasteita.

2.1 Määritelmä

Terminä "Internet of Things" on todennäköisesti peräisin vuodelta 1999 Kevin Ashtonin toimitusketjuja käsittelevän esitelmän otsikkona. Ashton näki jo 17 vuotta sitten ihmisten olevan rajoittuneita tuottamaan ja tallentamaan tietoa fyysisille esineille ja asioille perustuvasta ympäristöstään, minkä takia tietokoneiden tulisi kyetä tähän automaattisesti. Jos tietokoneet tietäisivät kaiken "esineistä", voitaisiin kaikkea toimitusketjuissa etenevää seurata ja laskea, jolloin niitä kyettäisiin tehokkaasti optimoimaan. Tämä Ashtonin esittämä määritelmä on hänen itsensä mukaan usein väärinymmärretty. (Ashton, 2009.)

Määritelmä onkin viime aikoina kasvanut kattamaan valtavan määrän erilaisia käyttötapoja ja muuttunut teknologian kehittyessä. Perusidea on kuitenkin pysynyt samana, eli tarkoituksena on yhä laittaa tietokoneet keräämään tietoa ympäristöstämme automaattisesti. Käyttömahdollisuudet Internetiä hyödyntävälle tietoa keräävien ja käyttävien esineiden verkolle ymmärretään siis nykyään huomattavasti laajemmin, kuin Ashton alun perin kaavaili. Niitä on esitetty muun muassa älykodin, -kaupungin ja terveydenhuollon kontekstissa. (Gubbi ym., 2013.)

Esineiden Internetin visioiden monimuotoisuus on seurausta termin kaksiosaisesta nimestä. Toisin sanoen termiä voidaan omien intressien mukaan lähestyä alkuperäisestä perspektiivistä, jossa keskiössä ovat verkkoon kytkeytyvät esineet tai Internetin näkökulmasta, jossa painotetaan esineiden Internetin verkkopuolta. Lisäksi kolmantena on olemassa semanttinen, termin molemmat puolet huomioon ottava näkökulma, jossa tärkeänä pidetään esimerkiksi kerätyn tiedon järjestelemistä ja varastoimista. Paradigmana esineiden Internet siis sisältää nämä kaikki kolme perspektiiviä. (Atzori ym., 2010.)

Tutkielmaa varten on valittu Gubbin ym. (2013) määritelmä, koska se ei keskity mihinkään tiettyihin protokolliin ja on useita määritelmiä käyttäjälähtöisempi. Määritelmässä huomioidaan myös kaikki mahdolliset esineiden Internetin käyttötavat. Vapaasti suomennettuna heidän määritelmänsä esineiden Internetille on:

> Yhteenliittymä aistivista ja aktuoivista laitteista, jotka kykenevät jakamaan tietoa alustojen välillä yhdistyneen viitekehyksen avulla, luoden yhteisen tilannekuvan, joka mahdollistaa innovatiivisia sovelluksia. Tämä saadaan aikaan saumattoman, ubiikin sensoritoiminnan, data-analytiikan ja tiedon esittämisen tavalla, jossa pilvilaskenta toimii yhdistävänä viitekehyksenä.

Miorandin ym. (2012) mukaan esineiden Internetin tutkimus on hyvin sirpaloitunutta ja on keskittynyt suureksi osaksi yksittäisiin teknologioihin ja käyttötapoihin. Heidän mukaansa tämä sirpaloituneisuus on vahingollista esineiden Internetin onnistuneelle käyttöönotolle. He painottavat tutkijoiden yhteistyön ja haasteiden ratkomista järjestelmätasolla, jotta esineiden Internetin tutkimus voisi tuottaa innovaatioita ja mahdollisuuksia toimialalla.

Joka tapauksessa esineiden Internet nähdään tutkimuksessa osana Internetin tulevaisuutta ja kehitystä. Miorandi ym. (2012) näkevät Internetin infrastruktuurin elintärkeänä perustana esineiden Internetissä liikkuvan tiedon jakamiselle ja leviämiselle. Se on heidän mielestään oleellinen, vaikka perinteinen käsitys Internetistä loppukäyttäjien päätelaitteiden välisenä infrastruktuuriverkkona katoaisikin. Frenchin ja Shimin (2016) mukaan esineiden Internet on osa yhteiskuntamme lähestyvää digitaalista mullistusta, jota edesauttaa 5G-teknologian mahdollistava ennennäkemätön yhdistettävyyden nopeus ja helppous. Tanin ja Wangin (2010) mukaan esineiden Internetin aikakausi tuo informaatio- ja viestintäteknologiaan kokonaisen uuden ulottuvuuden. Nykyään liitettävyyttä voi olla missä tahansa ja milloin tahansa, mutta tulevaisuudessa tähän voidaan lisätä mikä tahansa. Toisin sanoen kaikki esineet ovat yhdistettävissä.

2.2 Visio

Esineiden Internetin piirteisiin kuuluu verkkojen ja muun teknologian ubiikki läsnäolo (Gubbi ym., 2013; Miorandi ym., 2012; Atzori ym., 2010; Tan & Wang, 2010; French & Shim, 2016; Lin ym., 2017). Toisin sanoen esineiden Internetissä tietoa jatkuvasti keräävien, käyttävien ja jakavien esineiden sensorit ja aktuaattorit sekoittuvat ympäristöömme ja jatkuva teknologian läsnäolo katoaa käyttäjien tietoisuudesta (Gubbi ym., 2013). Esineiden keräämän massadatan (*engl. Big Data*) määrä tulee kasvamaan sitä mukaan, kun arkipäiväisiin esineisiin lisätään digitaalisia komponentteja ja niiden yhdistyneisyys toisiinsa sekä ihmisten välillä lisääntyy (French & Shim, 2016).

Älykkäät esineet ovat siis esineiden Internetin perusta. Miorandin ym. (2012) mukaan esineiden Internet rakentuu kolmelle esineiden ominaisuudelle: kaikkien esineiden tulee olla tunnistettavissa, kommunikoida ja olla vuorovaikutuksessa joko keskenään tai käyttäjien ja verkon muiden osien kanssa. He määrittelevät esineet fyysisiksi objekteiksi, joilla on oltava yksilöllinen tunniste, yhteys ainakin yhteen nimeen ja osoitteeseen, ainakin joitain kommunikaatio- ja tietojenkäsittelytoimintoja sekä mahdollisuus sensori- tai aktuaattoritoimintoihin. Heidän mukaansa sensorit ja aktuaattorit ovat se yksittäinen piirre, joka erottaa älykkäät esineet tavanomaisista verkon laitteista, eivätkä ne välttämättä edusta koko protokollapinoa, kuten nykyään vallitsevassa käsityksessä. Frenchin ja Shimin (2016) mukaan esineiden Internetiin liittyvien esineiden on lisäksi oltava käyttäjän ohjattavissa mistä ja milloin vain. Esimerkiksi älypuhelin edustaa heidän mukaansa älyteknologiaa, jolla tarkoitetaan kaikkea Internetiin yhdistettävää teknologiaa, mutta ei IoT-teknologiaa, koska käyttäjän on oltava läsnä laitetta käyttäessään. Gubbi ym. (2013) nimittävät älykkäiden esineiden yhteenliittymää älykkääksi ympäristöksi.

Järjestelmänä esineiden Internetin tulee tukea lukuisia ominaisuuksia, joista tunnistetaan tuki suurelle heterogeenisyydelle, koska IoT-laitteet ovat ominaisuuksiltaan ja käyttötavoiltaan hyvin monimuotoisia. Lisäksi tärkeää on skaalautuvuus, sillä monenlaisten arjen esineiden yhdistyessä Internetiin esineiden määrän tulee voida kasvaa ilman nimiavaruuksien loppumista tai ongelmia tiedon- ja palvelujen hallinnassa. Esineiden Internetin langattomuuden takia nousee tarve uusille radioteknologioille ja energiatehokkaille ratkaisuille, vaikka ongelma lieveneekin laitteiden tuottaessa energiaa omaan käyttöönsä esimerkiksi pienten aurinkopaneelien avulla. Esineitä sijaintia tulee voida seurata, varsinkin logistiikan sovelluksissa ja niiden pitää pystyä reagoimaan moniin tilanteisiin automaattisesti. Esimerkiksi niiden tulee kyetä muodostamaan tilapäisiä verkkoja, jotta ihmisen ei tarvitse jatkuvasti puuttua niiden toimintaan. Lisäksi dataa tulee käsitellä sopivissa ja standardoiduissa formaateissa massiivisten datamäärien käytön mahdollistamiseksi. Myös turvallisuus ja yksityisyys on otettava huomioon järjestelmätasolla. (Miorandi ym., 2012.)

Esineiden Internetin toiminta voidaan esittää yksinkertaistetusti siten, että tunnistetun esineen sensorin aistima data, kuten lämpötila, lähetetään edelleen

toiselle laitteelle tai järjestelmälle, joka sitten automatisoidusti käynnistää jonkin toiminnon, esimerkiksi ikkunan sulkemisen. Laitteessa tai järjestelmässä on mekanismi, jolla se voi lähettää palautteen käyttäjälle tai järjestelmänvalvojalle, josta järjestelmän tila ja toiminnan tulos käy ilmi. (Khan, Khan, Zaheer & Khan, 2012.) Esimerkki palautteesta voisi olla viesti "makuuhuoneen ikkuna suljettu" käyttäjän puhelimeen.

2.3 Arkkitehtuuri

Liitettävyyden saavuttaminen esineiden Internetissä vaatii useita ohjelmisto- ja laitteistokomponentteja monessa kerroksessa (Wortmann & Flüchter, 2015). Tan ja Wang (2010) toteavat, että 70-luvulle periytyvä nykyinen Internet-arkkitehtuuri ei sovellu sellaisenaan esineiden Internetille, koska sen alkuperäiset käyttötavat eroavat jo nykyisistäkin skenaarioista. Heidän mukaansa tämä alkaa ennen pitkää rajoittaa Internetin potentiaalia. Heterogeenisiä laitteita esineiden Internetissä voi olla jopa useita biljoonia, joten tarvitaan kipeästi joustavaa kerroksittaista arkkitehtuuria. Erilaisia arkkitehtuureja on esitetty useita, mutta tähän asti mikään niistä ei ole päätynyt vertailumalliksi. (Al-Fuqaha, Guizani, Mohammedi, Aledhari & Ayyash, 2015.)

Tavallisesti esitetty perustason malli jakaa IoT-arkkitehtuurin kolmeen kerrokseen (Al-Fuqaha ym., 2015; Lin ym., 2017; Wu, Lu, Ling, Sun & Du, 2010). Nämä kerrokset on nimetty havainto-, verkko- ja sovelluskerroksiksi (*engl. perception, network ja application layer*). Wun ym. (2010) mukaan esineiden Internetin arkkitehtuuri on yleisesti hyväksytty ja tämä kolmen tason malli hyvin tunnettu. Al-Fuqahan ym. (2015) mukaan se ei kuitenkaan vastaa oikeita IoT-ympäristöjä, koska esimerkiksi hyvin geneerisesti ilmaistu verkkokerros ei kata kaikkia käytettäviä teknologioita. Wun ym. (2010) mielestä kolmikerrosmallilla on merkitystä esineiden Internetin teknisen arkkitehtuurin ymmärtämisessä kehityksen alkuvaiheessa, mutta se ei voi selittää sen rakennetta kokonaisuudessaan.

Myös enemmän abstraktiota lisääviä malleja on esitetty, muun muassa Wun ym. (2010) ja Khanin ym. (2012) käyttämä viisikerroksinen malli (Al-Fuqaha ym., 2015). Tässä mallissa arkkitehtuuri esitetään esine-, lähetys-, palvelunhallinta-, sovellus- ja liiketoimintakerroksina.

Lisäksi on olemassa useasti esitetty palvelukeskeinen arkkitehtuuri (*engl. Service Oriented Architecture, SOA*), jossa esineiden ja sovellusten väliin esitetään lähetys-, palvelunhallinta- ja palvelun koostamiskerros (*engl. service composition layer*), viisikerrosmallista poiketen (Atzori ym., 2010; Lin ym., 2017; Tan & Wang, 2010). Al-Fuqahan ym. (2015) mukaan SOA ei sovellu esineiden Internetiin, koska kerrosten täytyy olla ajettavissa suorituskyvyltään rajallisilla laitteilla, mutta esimerkiksi palvelun koostamiskerros ei olisi tehokkaasti suoritettavissa. Viisikerroksinen arkkitehtuurimalli on heidän mielestään esitetyistä malleista soveltuvin esineiden Internetiin liiketoimintakerroksen ansiosta, jossa

suorituskykyä vaativat operaatiot voidaan suorittaa tehokkailla laitteilla. Viisikerroksinen malli on valittu tarkempaan tarkasteluun myös tätä tutkielmaa varten (ks. kuvio 1).

KUVIO 1 Esineiden Internetin arkkitehtuuri (Al-Fuqaha, 2015; Khan, 2012; Wu, 2010)

Arkkitehtuurissa alimpana sijaitseva esinekerros (*engl. objects layer*) edustaa fyysisiä laitteita eli esineitä ja niiden sensoreita. Tässä kerroksessa esineiden sensorit keräävät ja prosessoivat dataa, kuten esimerkiksi lämpötilaa, sijaintia ja kiihtyvyyttä. Kerätty data digitoidaan helposti käsiteltävään muotoon ja siirretään lähetyskerrokseen. (Al-Fuqaha ym., 2015; Khan ym., 2012; Wu ym., 2010.)

Lähetyskerroksen (*engl. transport layer*) päätehtävä on vastata esinekerroksessa tuotetun datan turvallisesta kuljettamisesta palvelunhallintakerrokseen (Al-Fuqaha ym., 2015; Khan ym., 2012; Wu ym., 2010). Dataa voidaan siirtää langattomasti tai langallisesti ja käytettävälle teknologialle on useita eri vaihtoehtoja (Khan ym., 2012; Wu ym., 2010).

Palvelunhallintakerros (*engl. service management layer*) parittaa palvelun ja sen pyytäjän (Al-Fuqaha ym., 2015). Tämä palvelunhallinta on tärkeää, koska esineiden Internetin laitteiden toteuttaessa erilaisia palveluja, tulee niiden olla yhteydessä vain samaa palvelua toteuttaviin laitteisiin (Khan ym., 2012). Tämä kerros vastaa myös saadun tiedon tallentamisesta, analysoinnista ja prosessoinnista sekä toimii päätöksentekijänä (Al-Fuqaha ym., 2015; Khan ym., 2012; Wu ym., 2010). Wun ym. (2010) mukaan palvelunhallintakerroksen kehittäminen on tärkeää massiivisten tietomäärien prosessoinnin hankaluuden takia.

Sovelluskerroksessa (*engl. application layer*) sijaitsevat esineiden Internetin älykkäät sovellukset ja niiden hallinta, mikä perustuu palvelunhallintakerroksessa prosessoituun tietoon (Khan ym., 2012). Esimerkkejä markkina-alueista ovat älykoti ja -terveydenhuolto (Al-Fuqaha ym., 2015; Khan ym., 2012). Nämä sovellukset ajavat esineiden Internetin laajempaa kehitystä (Wu ym., 2010).

Viimeiseksi liiketoimintakerros (*engl. business layer*) hallitsee kaikkia järjestelmän palveluita ja sovelluksia. Kerros hyödyntää sovelluskerroksesta saatua tietoa ja tuottaa esimerkiksi kuvaajia ja liiketoimintamalleja, jotta liiketoimintaa voidaan kehittää. (Al-Fuqaha ym., 2015; Khan ym., 2012; Wu ym., 2010.) Liiketoimintakerroksessa tapahtuu myös muiden kerrosten valvonta (Al-Fuqaha ym., 2015). Kerroksella on myös kuluttajien kannalta tärkeä rooli, sillä se vastaa käyttäjien yksityisyydenhallinnasta (Al-Fuqaha ym., 2015; Wu ym., 2010).

2.4 Teknologiat

Esineiden Internet tarvitsee toteutuakseen tukea innovatiivisista teknologioista (Tan & Wang, 2010). Miorandi ym. (2012) ennustavat, että esineiden Internetillä on edessään inkrementaalinen kehityksen tie, jossa olemassa oleviin järjestelmiin ja sovelluksiin lisätään vähitellen IoT-toiminnallisuutta. Heidän mukaansa mahdollistavien teknologioiden on aluksi tärkeää kyetä tunnistamaan älykkäät esineet ja mahdollistaa niiden vuorovaikutus ympäristön kanssa. Tutkimuksissa RFID eli Radio-Frequency IDentification nähdään tähän tarkoitukseen keskeisenä (Tan & Wang, 2010; Miorandi ym., 2012).

2.4.1 RFID

Esineiden Internetin ensimmäiset esinelähtöiset määritelmät juontavat juurensa juurikin RFID-teknologiaan. Avainkomponenteiksi kaavaillut RFID-järjestelmät koostuvat yhdestä tai useammasta lukijasta ja useasta RFID-tunnisteesta. Tunnisteet ovat jopa alle puolen millimetrin kokoisia antenniin yhdistettyjä, uniikilla tunnuksella varustettuja mikrosiruja, joita voidaan asettaa erilaisiin esineisiin tai ihmisiin ja eläimiin. RFID-lukijat tuottavat radiosignaalin, joka aktivoi tunnisteiden lähetyksen ja voivat siten etsiä tunnisteita langattomasti lähialueelta. (Atzori ym., 2010.)

RFID-teknologiaa on käytetty pääasiassa eristäytyneissä järjestelmissä esineiden tunnistamiseen ja seuraamiseen, eikä niiden käyttöä laajemmissa järjestelmissä ole täysin tutkittu (Miorandi ym., 2012). RFID-tunnisteita on kuvattu viivakoodin seuraajaksi, mutta kehittynyttä RFID-järjestelmää voi käyttää paljon muuhunkin kuin esineiden tunnistamiseen, kuten esineiden sijainti- ja tilatietojen saamiseen (Tan & Wang). Teknologian muihin etuihin lukeutuvat skannauksen nopeus, kestävyys, turvallisuus ja edullisuus, joista on hyötyä IoT-arkkitehtuurin alakerroksissa esineiden tunnistamisessa, seuraamisessa ja tiedon vaihtamisessa (Lin ym., 2017).

2.4.2 Langattomat sensoriverkot

Langattomat sensoriverkot (*engl. Wireless Sensor Network, WSN*) nähdään myös tärkeässä roolissa esineiden Internetissä (Lin ym., 2017; Gubbi ym., 2013; Atzori ym., 2010). Sensoriverkot koostuvat sensoreiden avulla aistivista, toistensa kanssa viestivistä solmuista (Atzori ym., 2010). WSN voi valvoa ja seurata laitteiden tilaa ja sensorien havaitsema tilatieto voidaan välittää verkossa eteenpäin "hyppien" solmulta toiselle, usein päätyen ohjauskeskukseen tai sink-nimellä kutsuttuun erikoissolmuun (Lin ym., 2017). Teknologian etuihin kuuluvat skaalautuvuus, pieni energiankulutus ja luotettavuus (Atzori ym., 2010; Lin ym., 2017). WSN-teknologialla on kuitenkin myös haasteita (Gubbi ym., 2013; Atzori ym., 2010). Atzori ym. (2010) mainitsevat näistä muun muassa nykyisen standardin (IEEE 802.15.4) liian pienen maksimaalisen pakettikoon.

Suhteessa RFID-teknologiaan, WSN on enemmän keskittynyt fyysisen maailman havaitsemiseen, kun taas RFID on enemmän käytetty esineiden tunnistamiseen, vaikka kumpaakin voidaan käyttää datan keräämiseen (Lin ym., 2017). Ne nähdäänkin toisiaan tukevina teknologioina (Atzori ym., 2010).

2.4.3 Verkkoteknologiat

Tan ja Wang (2010) huomauttavat, että esineiden yhdistämiselle on lukuisia langallisia tai langattomia tapoja, joista RFID ja WSN ovat vasta esimerkkejä. Esineiden keräämän datan välittämiseen voidaan käyttää laitteesta riippuen esimerkiksi WiFi-verkkoa, Bluetoothia tai matkapuhelinteknologiaa (Khan ym., 2013; Al-Fuqaha ym., 2015; Wu ym., 2010). Laitteiden osoitteiden hallintaan Internetprotokollan kuudes versio (IPv6) kasvatetulla osoiteavaruudellaan nähdään tarkoitukseen sopivana (Bandyopadhyay & Sen, 2011; Al-Fuqaha ym., 2015; Wu ym., 2010; LaBuda ja Gillespie, 2017).

Esineiden Internetin verkkokerrosten reitittämiseen ja datasiirron tukemiseen on jo esitetty monia protokollia, joista langattomiin likiverkkoihin (WPAN) kehitetty IEEE 802.15.4 on yksi esimerkki (Wu ym., 2017; Bandyopadhyay & Sen, 2011). Protokollan tarkoituksena on yhdistää lähiverkon laitteita matalalla energiankulutuksella, nopeudella sekä hinnalla (Wu ym., 2017). Se tarjoaa myös perustan monelle muulle langattomalle viestintäteknologialle. 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) puolestaan on protokolla, jonka avulla matalatehoisissa ja siten edullisissa likiverkoissa (*engl. low-power WPAN*) voidaan välittää IPv6-paketteja (Wu ym., 2017). Bandyopadhyayn ja Senin (2011) mukaan Internetprotokollan käyttöönotto älykkäissä esineissä, IEEE 802.15.4:n sisällyttäminen siihen ja 6LoWPAN:in käyttöönotto mahdollistaa esineiden Internetin laajamittaisen käyttöönoton.

2.4.4 Muita teknologioita

Pilvilaskentaa on ehdotettu ratkaisuksi esineiden Internetin tietojenkäsittelyä varten (Wu ym., 2010; Al-Fuqaha ym., 2015; Lin ym., 2017; Wortmann & Flüchter, 2015; Khan ym., 2013; Gubbi ym., 2013). Pilvilaskenta on jo kypsä teknologia ja suurin osa suurista IT-yrityksistä tarjoaa pilvipalveluita, joiden etuihin lukeutuvat tehokkuus, joustavuus sekä mahdollisuus datan tallentamiseen ja käyttämiseen (Lin ym., 2017). Lin ym. (2017), LaBuda ja Gillespie (2017) sekä Al-Fuqaha ym. (2015) ehdottavat perinteisen pilviteknologian tueksi sumu- tai reunalaskentaa (*engl. fog tai edge computing*), jossa pilvilaskentaa tuodaan tuoda lähemmäksi käyttäjiä kokonaan keskitetyn pilven sijaan. Sumu- tai reunalaskennassa pilveä hajautetaan tuomalla tietojenkäsittely- tai tallennuslaitteita verkon reunalle sen sijaan, että kaikki laskenta suoritettaisiin keskitetysti. Tämä tehostaisi esineiden keräämän datan tallennusta, prosessointia ja analysointia. (Lin ym., 2017.)

Tietojenkäsittelyyn voidaan toki käyttää perinteistäkin laitteistoa. IoT-sovelluksia varten kehitettyihin laitealustoihin kuuluu muun muassa Raspberry PI. Ohjelmistoalustoista IoT-skenaarioissa on käytetty Contiki RTOS -nimistä reaaliaikaista käyttöjärjestelmää (*engl. Real-Time Operating System, RTOS*), joka sisältää myös simulaattorin esineiden Internetin ja sensoriverkkojen simulointia ja emulointia varten. (Al-Fuqaha ym., 2015.) Bandyopadhyay ja Sen (2011) pitävät Contikia yhtenä lupaavimmista käyttöjärjestelmistä rajoittuneille laitteille.

2.5 Sovellukset

Esineiden Internetin sovelluksia on esitetty tutkimuksissa valtavasti. Esimerkkejä löytyy käytännössä kaikilta elämän alueilta ja toimialoilta. Miorandin ym. (2013) mukaan IoT-teknologia paitsi lisää kilpailua, myös yhdistää ennen erillisiksi ymmärrettyjä markkina-alueita sekä mahdollistaa kokonaan uusien syntymisen. Tässä kappaleessa on tutkielman kontekstin takia keskitytty esineiden Internetin sovelluksiin kuluttajan näkökulmasta. Sovellusten määrän takia tässä on esitelty niistä vain joitakin älykotiin ja -kaupunkiin sekä terveydenhuoltoon liittyen.

2.5.1 Älykoti

Lukuisat tutkimukset mainitsevat energiansäästön keskeisenä piirteenä älykodissa (Atzori ym., 2010; Gubbi ym., 2013; Miorandi ym., 2012; Khan ym., 2013; Lin ym., 2017). Kodin sensorit ja aktuaattorit mahdollistavat esimerkiksi sähkölaitteiden automaattisen sammuttamisen, kun ne eivät ole käytössä (Atzori ym., 2010; Miorandi ym., 2013). Sensorit voivat valvoa energian lisäksi muiden resurssien, kuten veden käyttöä ja myös tunnistaa käyttäjän tarpeet varmistaak-

seen, että esimerkiksi valojen ja lämmityksen säätäminen on hänen toiveidensa mukaista (Miorandi ym., 2013). Laitteet voivat myös käyttää energiaa älykkäästi sen ollessa halvimmillaan (Atzori ym., 2010).

Kodinkoneista esimerkiksi älykäs jääkaappi tai hylly voi skannata sisältämänsä tuotteiden RFID-tunnisteet ja auttaa esimerkiksi ostoslistan tekemisessä (Miorandi ym., 2013; Darianian & Michael, 2009). Tällaisessa kahden eri toimialan yhteistoiminnan esimerkissä yhteiset tekniset standardit ja rajapinnat ovat välttämättömiä (Miorandi ym., 2013). Darianianin ja Michaelin (2009) mukaan pesukone voi skannata vaatteiden RFID-tunnisteet ja valita oikean pesuohjelman.

Muita älykodin käyttökohteita ovat esimerkiksi älykkäät lukot ja muu kodin turvallisuudenhallinta (French & Shim, 2016). Esineet voivat esimerkiksi ilmoittaa käyttäjälle joutuessaan rajatun alueen ulkopuolelle (Atzori ym., 2010). Khanin ym. (2013) ja Atzorin ym. (2010) mukaan esineiden löytäminen helpottuu, kun käyttäjillä on pääsy tunnisteella varustetun esineen sijaintiin.

2.5.2 Älykaupunki

Älykaupunki tehostaa resurssien käyttöä samalla parantaen asukkaille suunnattujen palvelujen laatua. Esimerkiksi ilmanlaatua, melusaastetta yms. voidaan tarkkailla ja asukkaita tiedottaa reaaliaikaisesti. Älykäs valaistus mahdollistaa katuvalaistuksen optimoinnin ajankohdan, sään ja ihmisten läsnäolon mukaan sekä vikojen havaitsemisen. Katuvalojen lisääminen verkkoon mahdollistaa sivutuotteena myös laajemman WiFi-verkon tarjoamisen asukkaille. (Zanella, Bui, Castellani, Vangelista & Zorzi, 2014.)

Esineiden Internet tehostaa kaupungin liikenteenvalvontaa ja helpottaa siten reitin löytämistä. Sensorit tunnistavat myös vapaat pysäköintiruudut ohjaten autoilijat niihin, mikä nopeuttaa parkkipaikan etsintää. (Zanella ym., 2014, Miorandi ym., 2013.) Myös pysäköinnin valvonta tehostuu pysäköintiruutujen tunnistaessa pysäköintioikeuden tai sen puuttumisen esimerkiksi RFID:n avulla (Zanella ym., 2014). Lisäksi ajaminen helpottuu ja muuttuu turvallisemmaksi autojen ollessa yhteydessä tiehen ja ympäristöönsä. Autot voivat ajaa myös kokonaan itsenäisesti optimoiden esimerkiksi ajonopeuksia ja vähentäen ruuhkia. (Atzori ym., 2010; Lin ym., 2017.)

2.5.3 Terveys

Esineiden Internet tuo monia hyötyjä terveydenhuoltoon. Sensorit voivat esimerkiksi valvoa potilaiden terveydentilaa joko sairaalassa tai potilaan kotona. (Atzori ym., 2010; Gubbi ym., 2013; Miorandi ym., 2013; Bandyopadhyay & Sen, 2011; Khan ym., 2013.) Tarvittaessa tämä mahdollistaa nopean toiminnan potilaan terveydentilan heiketessä (Miorandi ym., 2013). Bandyopadhyayn ja Senin (2011) sekä Gubbin ym. (2013) mukaan tämä mahdollistaa iäkkään väestön kotona asumisen.

Miorandi ym. (2013) mainitsevat myös elämäntavan parantamisen puettavien (*engl. wearable*) sensorien avulla. Tämä mahdollistaa päivittäisten aktiviteettien seuraamisen sovelluksella ja antaa käyttäjälle ehdotuksia terveyshaittojen välttämiseksi.

2.6 Haasteet

Esineiden Internetin potentiaalin hyödyntämisen tiellä on kuitenkin vielä huomattavasti ratkaisemattomia haasteita. LaBudan ja Gillespien (2017) mukaan kolme kriittisintä haastetta liittyvät laitteiden yhteistoimintaan, massadataan ja turvallisuuteen.

Laitteiden kyky muodostaa yhteyksiä toisiinsa ja jakaa dataa mainitaan LaBudan ja Gillespien (2017) tutkimuksessa luultavasti tärkeimmäksi ja monimutkaisimmaksi esineiden Internetin ongelmaksi. Ongelmat näissä toiminnoissa johtuvat heidän mukaansa standardoinnin sekä yhteistyön puutteeseen laitteiden ohjelmistoissa ja viestintäprotokollissa. Myös Goad ja Gal (2017) tunnistavat standardien puutteen ongelmaksi, mikä johtaa arkkitehtuurin heterogeenisyyteen ja yhä teknologian käyttöönoton kallistumiseen. Nämä haasteet ovat seurausta valmistajien kilpailusta ja omien teknologioiden käytöstä (LaBuda & Gillespie, 2017; Khan ym., 2012).

Haasteita aiheuttavat myös IoT-laitteiden keräämät valtavat datamäärät (LaBuda & Gillespie, 2017; Goad & Gal, 2017; Chen, 2012). Chenin (2012) mukaan haasteena on datan älykäs jalostaminen viisaudeksi. Tämä on vaikeaa, koska kerätty data eroaa perinteisestä ihmisten tuottamasta datasta. Esimerkiksi iso osa datasta on turhaa tai epäluotettavaa ja sen tulisi usein olla käytettävissä reaaliaikaisesti. (Chen, 2012; LaBuda & Gillespie, 2017.) LaBuda ja Gillespie (2017) ehdottavat sumu- tai reunateknologiaa ratkaisuksi tietojenkäsittelyn haasteisiin.

Tässä tutkielmassa käsiteltävä haaste eli turvallisuus on yksi IoT:n tärkeimmistä ratkaistavista ongelmista (Bandyopadhyay & Sen, 2011; Khan ym., 2012; LaBuda & Gillespie, 2017; Goad & Gal, 2017; Chen, 2012; Miorandi ym., 2012). Turvallisuusstandardien puute asettaa datan turvallisuuden lisäksi käyttäjien yksityisyyden vaaraan, minkä takia turvallisuuden tulisi priorisoitua enemmän IoT-suunnittelussa (LaBuda & Gillespie, 2017). Gubbin ym. (2013) mukaan kryptografia on aina ensimmäinen puolustuskeino datan suojaamiseksi. Turvallisuuden takaaminen esineiden Internetissä on kuitenkin haastavaa esimerkiksi suorituskykyrajoitusten ja hinnan takia. Edullisten ja skaalautuvien kryptausalgoritmien kehittäminen on siksi tärkeää. (Chen, 2012; LaBuda & Gillespie, 2017.)

Esineiden Internetillä on edessään myös paljon käytännön haasteita, esimerkiksi laitteiden kestävyys. Laitteita otetaan käyttöön niin suuri määrä, että sensorien huolto voi koitua huomattavaksi menoeräksi, joten teknologian tulisi olla lähes tai kokonaan huoltovapaata. Lisäksi laitteiden akkujen tai paristojen

tulisi kestää riittävän kauan, etenkin jos niiden vaihtaminen myöhemmin on mahdotonta. Laitteiden pitäisi siis kyetä toimimaan vähällä energialla. (Chen, 2012.)

Energiankäyttöön liittyvät myös ympäristövaatimukset, joissa haasteena on tulevaisuuden IoT:n aiheuttama kasvava energiankulutus. Vihreät teknologiat voivat auttaa laitteiden mahdollisimman energiatehokkaassa toiminnassa. (Khan ym., 2012.)

3 ESINEIDEN INTERNETIN TURVALLISUUS

Tässä luvussa määritellään turvallisuus esineiden Internetin kontekstissa. Tässä tutkielmassa turvallisuudella tarkoitetaan ensisijaisesti kyberturvallisuutta perinteisen tietoturvallisuuden sijaan. Sen jälkeen esitellään kuluttajiin kohdistuvia turvallisuusuhkia sekä tapoja vastata näihin uhkiin esineiden Internetin turvallisuuden parantamiseksi.

3.1 Määritelmä

Von Solmsin ja Niekerkin (2013) mukaan termejä tietoturvallisuus ja kyberturvallisuus käytetään usein synonyymeinä. Kuitenkin perinteisen tietoturvallisuuden keskittyessä vain tietoresurssien suojaamiseen, menee kyberturvallisuus astetta pidemmälle ja huomioi muun muassa turvallisuuden inhimillisen puolen laajemmin (von Solms & Niekerk, 2013).

Kyberturvallisuus pyrkii palveluiden saatavuuteen, datan eheyteen ja luottamuksellisuuteen, mitkä ovat varsin yhteneväisiä tietoturvallisuuden tavoitteiden kanssa. Nämä kaksi termiä ovatkin osittain päällekkäisiä, mutta varsinainen ero ilmenee siinä, että tietoturvallisuus käsittää kaikki tietoresurssit, myös ei-kyberympäristöön tallennetut. Kyberturvallisuus puolestaan keskittyy nimensä mukaisesti vain kyberympäristöihin, mutta käsittää turvallisuuden laajemmin. Kyberturvallisuus sisältää myös ne asiat, jotka ovat ICT:n välityksellä haavoittuvaisia, mutta eivät tietoresursseja. Esimerkiksi kodinkoneisiin käsiksi pääsy verkon välityksellä voidaan käsittää kyberturvallisuuteen kuuluvaksi riskiksi. (von Solms & Niekerk, 2013.) Suuri osa esineiden Internetin turvallisuusuhkista sijaitsee siten tietoturvallisuuden piirin ulkopuolella.

Esineiden Internetin turvallisuudesta puhuttaessa tavoitteet ovat pitkälti samoja, kuin kyberturvallisuudessa perinteisen Internetin kontekstissa. Chadidin, Benabdellahin ja Azizin (2017) mukaan myös esineiden Internetin turvalli-

suuden kolme pilaria ovat luottamuksellisuus (*engl. confidentiality*), eheys (*engl. integrity*) ja saatavuus (*engl. access*). Luottamuksellisuus pyrkii estämään käyttäjien datan varastamisen ja eheys niiden oikeudettoman muokkaamisen. Saatavuus pyrkii turvaamaan käyttäjän pääsyn hallitsemaansa dataan. (Chadid ym., 2017.) Dhillonin, Carterin ja Abedin (2016) tutkimuksessa määritellään tarkemmin neljä perustavoitetta esineiden Internetin turvaamiseksi: henkilökohtaisen datan turvaaminen yleisissä tietokannoissa, eettisen toiminnan kehittäminen ja ylläpito, datan eheys sekä pääsynhallinta. Nämä tavoitteet ovat hyvin yhteneväisiä aiemmin mainittujen pilarien kanssa, eettisyyttä lukuun ottamatta. Tällä tarkoitetaan eettisten ja vastuullisten toimintatapojen luomista IoT-ympäristössä.

Kuluttajakontekstissa erityisen tärkeä tavoite on käyttäjien yksityisyys, joka on noussut huolenaiheeksi esineiden Internetiin kuuluvan käyttäjille näkymättömän tiedonkeruun, -käytön ja -jakamisen takia. Yksityisyydellä tarkoitetaan paitsi henkilökohtaisen varastoidun sekä siirrettävän datan suojaamista, myös suojaa ruumiilliselta vahingolta ja alueellisilta loukkauksilta. (Aleisa & Renaud, 2017.) Yksityisyyteen liittyy lisäksi käyttäjän mahdollisuus hallita omia tietojaan (Weber, 2010; Aleisa & Renaund, 2017). Monet tunnetuista esineiden Internetin turvallisuusuhkista kohdistuvat käyttäjien henkilökohtaisten tietojen saamiseen ja väärinkäyttöön (Porras ym., 2018).

Esineiden Internetin turvallisuusvaatimukset palveluiden saatavuuden ja luotettavuuden osalta ovat suurempia kuin perinteisessä Internetissä sen sovellusten sijaitessa yhä kriittisimmillä alueilla, kuten terveydenhuollossa ja liikenteessä (Suo, Wan, Zou & Liu, 2012). Näillä aloilla seuraukset kuluttajille turvallisuustoimien pettäessä voivat olla jopa hengenvaarallisia esimerkiksi hyökkääjän vahingoittaessa auton jarruja (Atamli & Martin, 2014). Solms ja Niekerk (2013) mainitsevat kyberterrorismin mahdollistavan vieläkin vakavammat seuraukset kriittiseen infrastruktuuriin iskemällä. Weberin (2010) mukaan esineiden Internetin tulee kyetä vastustamaan hyökkäyksiä sopeutumalla yksittäisten solmujen pettämiseen. Tällainen kyky epäilemättä lievittää yksittäisten hyökkäysten vaikutusta koko järjestelmään.

Esineiden Internet on kuitenkin erityisen haavoittuvainen kyberuhkille moninaisista syistä. Esineet ovat itsessään haavoittuvaisia hyökkäyksille, koska ne kulkeutuvat julkisiin tiloihin, viestivät langattomasti ja ovat yhteyksissä toisiinsa (Sicari ym., 2015). Esineiden valtava määrä johtaa haasteisiin laitteiden tunnistamisessa ja todentamisessa, jolloin järjestelmän datavirran sisällöstä ei voida olla varmoja. Lisäksi rajoitukset laitteiden suorituskyvyssä, akkuvirrassa ja muistissa sekä niitä yhdistävän verkon rajoitukset liikkuvuudessa, koossa ja heterogeenisyydessä aiheuttavat rajoitteita turvallisuudelle. Esineiden riippuvuus toisten laitteiden toiminnasta voi aiheuttaa lisää riskejä. Esimerkiksi ilmastointilaitteen pettäminen voi aiheuttaa lämpötilan nousun ja siten ikkunan automaattisen avautumisen, altistaen rakennuksen murrolle. IoT-laitteiden valmistajien on todettu laiminlyövän jopa perustason turvallisuusmekanismeja, kuten salasanoja. Huolta aiheuttaa myös näiden haluttomuus tai kyvyttömyys päivittää laitteidensa ohjelmistoja. (Porras ym., 2018.) Jo aiemmin mainittu val-

mistajien haluttomuus yhteistyöhön johtaa turvallisuusongelmien ehkäisemiseksi ja ratkaisemiseksi tehtävän työn hajaantumiseen (Covington & Carskadden, 2013). Weberin (2010) mukaan esineiden Internetin turvallisuutta ei ole huomioitu riittävästi lainsäädännössä ja valmistajien toteuttama itsesääntely ei riitä vakuuttavan turvallisuusratkaisun toteuttamiseen.

3.2 Esineiden Internetin turvallisuusuhat

Esineiden Internetin käyttäjien turvallisuuteen ja yksityisyyteen kohdistuvilla uhkilla on kolme pääasiallista lähdettä: muut käyttäjät, laitevalmistajat ja ulkoinen osapuoli. Muut käyttäjät voivat hyödyntää omistamiensa laitteiden haavoittuvuuksia esimerkiksi hyökkäysten toteuttamisessa samankaltaisiin järjestelmiin. Valmistajilla on mahdollisuus väärinkäyttää teknologiaa esimerkiksi käyttäjien tietoja keräämällä ja myymällä. Ulkoiset osapuolet voivat tunkeutua järjestelmään paitsi käyttäjien tietojen toivossa, myös esimerkiksi taloudellista haittaa tai muuta vahinkoa aiheuttaakseen. (Atamli & Martin, 2014.) Tämän luvun tarkoituksena on tunnistaa esineiden Internetissä kuluttajiin kohdistuvat turvallisuusuhat, jotka ovat pääosin erilaisia kyberhyökkäysmalleja.

3.2.1 Solmuihin kohdistuvat hyökkäykset

Esineiden Internetin verkko koostuu useasta solmusta, joihin hyökkääjät voivat iskeä monin tavoin. Solmun kaappauksella (*engl. node capture*) viitataan hyökkäykseen, jossa pyritään ottamaan verkon solmu tai muu infrastruktuurin osanen, kuten tietovaranto haltuun (Roman, Zhou & Lopez, 2013). Tämä voi tapahtua solmun laitteistoon kajoamalla tai korvaamalla koko solmu toisella. Hyökkääjät pystyvät sitten paljastamaan solmun sisältämän tiedon, mukaan lukien erilaiset avaimet. Nämä avaimet voidaan kopioida toiseen solmuun, joka sitten esittää turvallista solmua, mutta onkin todellisuudessa hyökkääjien hallinnassa ja siten haitallinen. Tällaista variaatiota kutsutaan solmun kopioimiseksi (*engl. node replication*).

Haitallista solmua voidaan käyttää muun muassa replay-hyökkäykseen, jossa isäntäsolmun jo aikaisemmin vastaanottama tunnistetieto lähetetään sille uudelleen, mutta tällä kertaa hyökkääjän laitteesta. Hyökkääjä voi siten saavuttaa järjestelmän luottamuksen. Onnistuessaan hyökkäys rikkoo sertifioinnin pätevyyden. (Zhao & Ge, 2013; Lin ym., 2017; Chadid ym., 2017.)

Solmuja voidaan myös saastuttaa injektoimalla niihin haitallista koodia tai väärennettyä dataa. Haitallista koodia voi käyttää yksittäisten solmujen hallintaan tai jopa laajemman järjestelmän haltuunottoon. Väärennetty data voi kulkeutua edelleen sovelluskerrokseen ja aiheuttaa väärien toimintojen tai palvelujen suorittamisen. (Lin ym. 2017.) Esimerkiksi IoT-teknologiaa hyödyntävä ajo-

neuvo voi joutua hyökkääjän hallintaan tai väärennetty data aiheuttaa sen luulemaan, että tiellä on jokin este, mikä johtaisi sen automaattiseen jarruttamiseen.

Haitalliset solmut voivat uhata koko verkon turvallisuutta myös kuluttamalla solmujen rajallista energiaa suunniteltua enemmän. Solmujen energian loppuminen voi johtaa jopa koko verkon tuhoutumiseen (Zhao & Ge, 2013; Chadid ym., 2017; Lin ym., 2017). Lin ym. (2017) nimittävät tämän tämäntyyppisiä hyökkäyksiä univajehyökkäyksiksi (*engl. sleep deprivation attack*), koska solmut ovat usein suunniteltuja seuraamaan "unirytmiä" säästääkseen energiaa. Univajehyökkäys toisin sanoen rikkoo tämän rutiinin esimerkiksi jatkuvasti herättämällä solmuja, johtaen lopulta solmujen sammumiseen.

Verkon solmuista etenkin yhdyskäytäväsolmut (*engl. gateway node*) ovat ongelmallisia, sillä ne voivat hyökkäyksen tapahtuessa vuotaa kaikki hyökkääjien tarvitsemat tiedot verkkoon liittyen (Chadid ym., 2017). Solmut ja esineiden Internetiä koostavat järjestelmät ovat yleisestikin haavoittuvaisia, koska solmujen ubiikkius ja ripottelu ympäristöön tuovat ne lähemmäksi potentiaalisia hyökkääjiä (Covington & Carskadden, 2013).

3.2.2 Salauksen murtaminen

Hyökkääjä voi käyttää monia eri metodeja salauksen eli kryptauksen murtamiseen järjestelmässä. Kryptoanalyysillä (*engl. cryptanalysis*) tarkoitetaan keinoja, joilla pyritään salausavaimen ratkaisemiseen salatun tai salaamattoman tekstin perusteella. Perinteinen kryptoanalyysi ei kuitenkaan ole kovin tehokasta, joten sen rinnalla voidaan käyttää ns. side channel-hyökkäyksiä (*engl. side channel attack, SCA*). (Lin ym., 2017.) Niissä järjestelmää tarkastellaan laajemmin ja yritetään siitä poimitun tiedon perusteella auttaa avaimen ratkaisemisessa. Tiedot perustuvat muun muassa aikaan, joka kuluu salausalgoritmin suorittamiseen, virrankulutukseen ja vapautuvaan elektromagneettiseen säteilyyn. (Zhao & Ge, 2013; Lin ym., 2017; Chadid ym., 2017; Atamli & Martin, 2014.) Etenkin virrankulutuksen tarkkailuun perustuva differentiaalinen tehoanalyysi (*engl. differential power analysis, DPA*) on tehokas hyökkäyksen muoto (Zhao & Ge, 2013).

Salauksella pyritään estämään hyökkääjää kaappaamasta selkokielistä signaalia. Signaalit esineiden Internetissä ovat yleensä langattomia, joten niiden salakuuntelu on verrattain helppoa. (Lin ym., 2017.) Rajoitukset laitteistossa voivat kuitenkin estää järjestelmää käyttämästä tehokasta salausalgoritmia. Samaan aikaan tietoa voidaan joutua välittämään lyhyinä purskeina tietyssä standardimuodossa. Purskeiden tiheys ja standardiformaatin käyttö saattaa helpottaa kryptoanalyysissä, mutta toisaalta myös hyökkääjän kerrallaan kaappaama tietomäärä on pienempi. (Covington & Carskadden, 2013.) Joka tapauksessa selkokielisen signaalin kaapattuaan hyökkääjä voi saada käyttäjän laitteesta luottamuksellista tietoa tai rikkoa tämän yksityisyyttä.

3.2.3 Palvelunestohyökkäys

Palvelunestohyökkäykset (*engl. Denial of Service, DoS*) ovat yleisimpiä hyökkäyksiä sensoriverkoissa ja Internetissä (Zhao & Ge, 2013). Nimensä mukaisesti niillä pyritään estämään palvelujen tarjoaminen verkkoresursseja ylirasittamalla (Zhao & Ge, 2013; Roman ym., 2013; Chadid ym., 2017). Romanin ym. (2013) mukaan hyökkäys voidaan kohdistaa paitsi palveluntarjoajaan, myös langattomaan viestintäinfrastruktuuriin itseensä, tavoitteena viestintäkanavien häirintä. DoS-hyökkäyksille on olemassa useita valmiita kaavoja, kuten Ping of Death ja TearDrop (Lin ym., 2017).

Atamli ja Martin (2013) sekä Roman ym. (2013) näkevät fyysisen laitteisiin kajoamisen yhtenä DoS-hyökkäyksen muotona. Laite voidaan esimerkiksi varastaa tai tuhota. Esineiden Internetin laitteet tai niiden komponentit voivat olla helposti hyökkääjien ulottuvilla. Palvelunestohyökkäyksiä voi siis esiintyä sekä esine- että verkkokerroksissa (Chadid ym., 2013).

Luonnollisesti palvelunestohyökkäyksen vaikutus käyttäjien turvallisuuteen voi olla IoT-kontekstissa huomattava. Esimerkiksi mahdollisissa sovelluksissa mainitun terveydenhuollon etävalvontajärjestelmän toiminnan estäminen voisi johtaa siihen, että potilaalle ei kyetä tarjoamaan hoitoa sitä tarvitessaan.

3.2.4 Man-in-the-Middle -hyökkäys

Man-in-the-Middle -hyökkäyksessä (MitM) kahden normaalin, kommunikoivan laitteen välissä on kolmas laite, joka välittää ja esimerkiksi tallentaa laitteiden välillä liikkuvan tiedon. Normaalit laitteet kuitenkin luulevat kommunikoivansa suoraan toistensa kanssa. Ne eivät kykene havaitsemaan kolmannen laitteen olemassaoloa, koska se kaappaa näiden tunnistetiedot. Hyökkäystä voidaan käyttää paitsi tiedon salakuunteluun ja varastamiseen myös yhteyden häirintään ja hallintaan. Se siis vaarantaa tiedon luottamuksellisuuden, eheyden ja yksityisyyden. (Lin ym., 2017.)

Hyökkäys on erityisesti uhka esineiden Internetissä, koska sen valtava populaatio kasvattaa verkon yhteistoimivuutta ja siten mahdollisten yhteyksien määrää, jotka voivat olla vaarassa joutua Man-in-the-Middle -hyökkäyksen uhriksi. Lisäksi esineiden Internetin liikkuvuus ja hajautuneisuus helpottaa hyökkäyksen toteuttamista ilman kiinnijäämisen riskiä (Covington & Carskadden, 2013). Suo ym. (2012) väittävät, että vaikka IoT-arkkitehtuurin verkkokerroksella onkin verrattain kokonaisvaltaiset turvallisuusominaisuudet ja suojautumiskyvyt, MitM-hyökkäysten mahdollisuus on silti otettava huomioon.

3.2.5 Muut verkkohyökkäykset

Esineiden Internetin verkkokerroksissa esiintyy DoS- ja MitM-hyökkäysten muitakin hyökkäystyyppejä. Datamanipulointi (*engl. spoofing*) viittaa varastettujen pääsy- tai tunnistetietojen käyttämistä pääsyn saamiseksi palveluun tai jär-

jestelmään. (Lin ym., 2017; Atamli & Martin, 2014.) Palvelusta riippuen tällä voi olla vakaviakin seurauksia, esimerkiksi käyttäjän asunnon oven avaaminen. Pääsytiedot voivat olla peräisin laitteesta itsestään, kaapattu signaalista tai saatu tietojenkalastelulla (Atamli & Martin, 2014). Lin ym. (2017) mainitsevat erikseen IP- ja RFID-manipuloinnin. Hyökkääjä voi siis käyttää luotetulta laitteelta saatua IP-osoitetta tai RFID-tunnisteen tietoja lähettääkseen haitallista dataa järjestelmään.

Lin ym. (2017) kirjoittavat myös sensoriverkoissa tapahtuvista sinkhole- ja wormhole-hyökkäyksistä. Sinkhole-hyökkäyksessä haitallinen solmu viestittää muille solmuille omaavansa hyvät virta-, tiedonkäsittely- tai viestintäominaisuudet. Silloin viereiset laitteet suosisivat sitä lähettäessään dataa eteenpäin sensoriverkossa. Hyökkääjä voi siten saada luottamuksellista tietoa haltuunsa tai käyttää solmua muiden hyökkäysten, kuten palvelunestohyökkäyksen valmisteluun. Myös wormhole-hyökkäyksiä esiintyy sensoriverkoissa. Siinä kaksi eri paikoissa sijaitsevaa, haitallista solmua luovat välilleen yhden hyppäyksen pituisen hypyn, vaikka todellinen reitti niiden välillä olisi huomattavasti useamman hypyn pituinen. Hyppyjen vähetessä enemmän dataa kulkee haitallisten solmujen kautta ja johtaa samanlaisiin seurauksiin kuin sinkhole-hyökkäys. (Lin ym., 2017.)

3.2.6 Ylempien kerrosten uhat

Myös korkeammalla tasolla IoT-arkkitehtuurissa esiintyy kyberuhkia, jotka kerroksen roolin takia kohdistuvat sovelluksiin ja niiden käyttäjiin. Tietojenkalastelu (*engl. phishing*) on esimerkki tällaisesta uhasta, jolla tarkoitetaan luottamuksellisen tiedon haalintaa käyttäjiltä useimmiten sähköpostien ja tekaistujen verkkosivujen avulla. (Lin ym., 2017; Gupta, Nalin, Arachchilage & Psannis, 2018.) Guptan ym. (2018) mukaan IoT-laitteita voidaan käyttää bottiverkkona kalastelusähköpostien välittämiseen, minkä vuoksi ne tulisi kyetä estämään heti alkuunsa. Haasteita tuottaa kuitenkin viestien tunnistaminen ja suodattaminen, eikä tähän ole kehitetty ratkaisua IoT-kontekstissa. Linin ym. (2017) mukaan paras ratkaisu tietojenkalasteluun on käyttäjän valppaus, mutta laitteilta kalastelun tunnistaminen vaatii älykkyyttä, jollaista niillä ei välttämättä ole.

IoT-sovellukset ovat perinteisten Internet-sovellusten tavoin alttiita muillekin tavanomaisille uhkille, kuten viruksille ja muille haittaohjelmille. Esimerkkejä viruksista ovat troijalaiset ja madot, jotka voivat varastaa tai muokata luottamuksellista dataa. (Lin ym., 2017.) Haittaohjelmat voivat aiheuttaa massiivista vahinkoa esimerkiksi älykaupungin tai -infrastruktuurin kontekstissa, mistä todisteena on Stuxnet-virus, jota käytettiin iranilaisen ydinvoimalaitoksen laitteiston tuhoamiseen vuonna 2010 (Chadid ym., 2017). Isku sähköverkkoon voi keskeyttää sähkönjakelun laajalla alueella, kuten Ukrainassa vuonna 2015, joka oli ensimmäinen kyberhyökkäyksen aiheuttama sähkökatkos (Liang, Weller, Zhao, Luo & Dong, 2016). Liangin ym. (2016) mukaan tässä hyökkäyksessä hyödynnettiin useita erilaisia keinoja, mukaan lukien tietojenkalastelua, palve-

lunestohyökkäystä ja haittaohjelmia. Hyökkäys johti sähkönjakelun häiriintymiseen yli 200 000 asiakkaalta useiden tuntien ajaksi. Vastaavia iskuja voi pitää mahdollisena myös esineiden Internetissä, jos sähköverkko tuodaan osaksi sitä.

Yläkerroksissa on myös monia dataan liittyviä uhkia. Kykenemättömyys käsitellä valtavia tietomääriä voi johtaa verkon tukkeutumiseen ja datan menetykseen (Zhao & Ge, 2013; Chadid ym., 2017). Datan käsittelyyn liittyvät myös sen suojauksen prosessoinnin algoritmien heikkoudet, jotka voivat aiheuttaa kuluttajien yksityisen datan vuotamista (Zhao & Ge, 2013; Chadid ym., 2017). Linin ym. (2017) mukaan datan yksityisyyden takaamisessa haasteena on kehittää sellaisia järjestelmiä, jotka kykenevät sekä datan tehokkaaseen hyödyntämiseen että yksityisyyden turvaamiseen. Yksityisyyden säilyttäminen datan koostamisessa voi perustua anonyymiyteen, salaukseen tai perturbaatioon, ts. häiriöön. Perturbaatiossa dataa muokataan, jaetaan ja siihen lisätään häiriötä, saaden aikaan yksityisyyden säilymisen. Perturbaatio onkin ollut suosittu tapa esineiden Internetissä sen suorituskyvyn takia, mutta se johtaa usein datan hyödyllisyyden laskemiseen. Anonyymiyteen perustuvat tavat ovat puolestaan haavoittuvaisia tietoliikenneanalyysille ja olemassa olevat salausmenetelmät toimivat vain dataa siirrettäessä.

3.3 Esineiden Internetin turvallisuusratkaisut

Turvallisuusvaatimusten täyttäminen ja siten turvallisuuden takaaminen esineiden Internetin käyttäjille edellyttää siis hyvin laajaan uhkien kirjoon vastaamista erilaisin turvatoimin. Uhkien tapaan turvallisuusratkaisuja on esitetty arkkitehtuurin kaikissa kerroksissa. Tutkimuksissa tunnistetut ratkaisut eivät ole myöskään täysin teknisiä, vaan osa niistä liittyy esimerkiksi käyttäjien turvallisuustietoisuuden nostamiseen.

3.3.1 Todentaminen

Suon ym. (2012) mukaan solmujen todentaminen on välttämätöntä, jotta luvaton pääsy niihin voidaan estää. Esineiden Internetiin soveltuvia todentamismalleja on olemassa lukuisia. Zhangin, Chengin ja Shiehin (2016) mukaan esineiden Internetiin soveltuvassa vieraiden laitteiden todentamisessa voidaan käyttää muun muassa porttikäytävää tai turvallisuusmerkkiä (*engl. security token*). Ensimmäisessä tavassa verkon porttikäytävä tunnistaa verkkoon liittyvän vieraan laitteen salasanan tai vastaavan perusteella. Todennus toistetaan aina ennen uuden viestintäistunnon aloittamista. Hyviin puoliin lukeutuu se, että vieraat laitteet voidaan todentaa itsenäisesti verkon sisäisiin verrattuna eli esimerkiksi kodin laitteet voidaan todentaa perinteisesti. Tehokkaan porttikäytävän käyttö todentamisessa toisaalta parantaa suojausta, mutta se voi samalla muodostua verkkoliikenteen pullonkaulaksi ja lisäksi sen turvallisuuden pettäminen aset-

taa kaikki muut laitteet alttiiksi uhkille. Toisessa tavassa vieraat laitteet tunnistetaan myös porttikäytävän avulla, mutta salasanan sijaan käytetään tietyn ajan voimassa olevaa turvallisuusmerkkiä. Merkki voi siis olla voimassa useamman istunnon ajan. Tämä vapauttaa porttikäytävän rasitusta ja on muutenkin kevyempi laitteistolle. Porttikäytävän pettäminen on kuitenkin yhtä lailla uhka kuin edellisessäkin tavassa ja lisäksi merkkien käyttö voi olla yksinkertaisia salasanoja mutkikkaampaa. (Zhang ym., 2016.) Todennuksessakin on siis huomioitava laitteiden rajoitukset ja muut käyttökohteen erityispiirteet eli yhtä oikeaa tapaa ei ole kehitetty.

3.3.2 Luottamus

Useat tutkimukset mainitsevat luottamuksen oleellisena esineiden Internetin turvallisuuden parantamiselle. Sicarin ym. (2015) mukaan perinteiset pääsynhallintamallit eivät välttämättä ole käyttökelpoisia hajautetussa esineiden Internetissä, jossa solmujen identiteettejä ei tunneta etukäteen. Pääsynhallinnassa voitaisiin hyödyntää luottamus- ja pehmolaskentaperusteista mallia, jossa laitteiden väliset luottamussuhteet vaikuttaisivat niiden yhteistoimintaan. Esimerkiksi Fuzzy approach to the Trust Based Access Control (FTBAC) -niminen malli käyttäisi laskettuja luottamuspisteitä laitteille perustuen kokemukseen, tietämykseen ja suosituksiin. Pisteet heijastuvat sitten laitteen saamiin valtuuksiin ja pääsyn antamiseen ja epäämiseen. Toisiinsa luottavat laitteet suosivat toisiaan muita laitteita enemmän vaihtaessaan erilaisia resursseja ja palveluita.

Zhang ym. (2015) esittävät tutkimuksessaan aiemmin mainittujen todennusmallien lisäksi kaksi luottamukseen perustuvaa mallia: luottamusketju ja luottamuspuu. Näissä malleissa vieraat solmut todennetaan viittaamalla jo luotettuihin solmuihin. Pääasiallinen ero luottamusketjulla ja -puulla on niiden koossa, ketju toimii rajoitetummassa ympäristössä puun ollessa globaali kokonaisuus. Luottamusketjut ovat sekä tehokkaita että varmoja, mutta myös monimutkaisia toteuttaa ja joustamattomia, koska kaikki laitteet tulisi todentaa samalla tavalla. Globaali luottamuspuu olisi hyvin luotettava ja toteuttaisi globaalia standardia, soveltuen siten kaikkien laitteiden yhteiseen todentamiseen. Se ei kuitenkaan ole toteutettavissa nykyisessä Internetissä ja olisi joka tapauksessa kallis.

Luottamuksella on merkitystä myös muissa esineiden Internetin suhteissa. Käyttäjien luottamus IoT-järjestelmään auttaa heitä pääsemään yli epävarmuudesta ja riskeistä. Luottamus arkkitehtuurin kerrosten välillä tarkoittaa viestinnän turvallisuutta ja yksityisyyttä. Konseptina luottamus käsittääkin sekä turvallisuus- että yksityisyysnäkökulman. (Porras ym., 2018.)

Luottamuksen tuottamisessa voidaan käyttää erilaisia mekanismeja. Dhillon ym. (2016) mainitsevat organisaatioiden vastuun luottamuksen aikaansaamisessa. Tämä voi tapahtua esimerkiksi päivittämällä tuotteita tiheästi tuoreimpia hyökkäyksiä vastaan ja valvomalla järjestelmää aktiivisesti. Myös Lin

ym. (2017) peräänkuuluttavat luottamuksenhallintajärjestelmän suunnittelemista ja käyttöönottamista luottamuksen saavuttamiseksi.

3.3.3 Salaus

Datan tehokas salaus on ehdottoman tärkeää tiedon luottamuksellisuuden turvaamiseksi, mutta samaan aikaan salausteknologian tulisi olla mahdollisimman kevyttä laitteistolle tarpeettoman resurssien kulutuksen välttämiseksi (Suo ym., 2012). Katagin ja Moriain (2008) mukaan Lightweight Cryptography (LWC) on esineiden Internetiin hyvin soveltuva tekniikka, joka tarkoittaa erityisesti rajoitetuille ympäristöille suunniteltua salausalgoritmia tai -protokollaa.

Suon ym. (2012) mukaan perinteisesti verkkokerroksessa käytetään by-hop -salausta, jossa data salataan vain välittävien solmujen sitä siirtäessä ja sovelluskerroksessa end-to-end -salausta, jossa data salataan lähettäjältä vastaanottajalle koko prosessin ajan. Salausmekanismi esineiden Internetissä tulisi heidän mukaansa valita käyttökohteen mukaan siten, että turvallisuusvaatimusten ollessa korkeita, tulisi valita end-to-end -salaus. Muussa tapauksessa toimisi by-hop -salaus, joka vaatii korkean luottamuksen välittäviin solmuihin, mutta on toisaalta end-to-end -salausta nopeampi, edullisempi ja tehokkaampi. (Suo ym., 2012.)

Laitteiden välisen kommunikoinnin turvaamiseksi voidaan Porraksen ym. (2018) mukaan käyttää perinteisten turvallisuusratkaisujen lisäksi IoT-keskeisiä käytäntöjä. Nguyen, Laurent ja Oualha (2015) esittelevät kahden laitteen välisen yhteyden salaamiseen kaksi pääasiallista tyyppiä: epäsymmetrisen eli julkisen avaimen salaus (engl. asymmetric key) ja etukäteen jaettavan symmetrisen avaimen salaus (engl. symmetric key pre-distribution). Epäsymmetrisen avaimen salauksessa viestin salaamiseen ja purkamiseen käytetään eri salausavainta, kun taas symmetrisessä käytetään etukäteen jaettua tai arvottua avainta, jota käytetään sekä salaamiseen että purkamiseen. Epäsymmetrinen salaus on käytössä perinteisessä Internetissä, mutta se vaatii usein paljon suorituskykyä ja energiaa eri salaustoimenpiteiden määrän takia. (Nguyen ym., 2015.) Zhaon ja Gen (2014) mukaan symmetrinen salaus voisi sopia hyvin sensoriverkkoihin, joissa yksittäisten solmujen prosessointikyky on heikko. Toisaalta sittemmin on kehitetty myös rajoitettuihin ympäristöihin soveltuvia epäsymmetrisiä ratkaisuja. Niiden optimointi on yksi vaihtoehto esineiden Internetiin soveltuvien salausvaihtoehtojen joukosta, olemassa olevien protokollien räätälöinnin ja erilaisten hybridiratkaisujen ohella. (Nguyen ym., 2015.)

Side channel -hyökkäyksiin kuuluvan differentiaalisen tehoanalyysin torjumiseen on kaski pääasiallista lähestymistapaa: piilottaminen (*engl. hiding*) ja peittäminen (*engl. masking*). Piilottaminen tähtää datan ja energiankulutuksen yhteyden poistamiseen analyysin vaikeuttamiseksi. Peittäminen puolestaan perustuu salauslaitteiden välittäjäarvojen arpomiseen. (Zhao & Ge, 2013.)

3.3.4 Verkon turvallisuus

IoT-laitteista koostuvien verkkojen turvallisuuden parantamiseksi on tutkimuskirjallisuudessa esitetty perinteisiä sekä joitakin erityisesti esineiden Internetiin soveltuvia keinoja. Romanin ym. (2013) mukaan miljardien esineiden verkoissa vikasietoisuus on erityisen tärkeää, koska laitteet voivat vikaantua, rikkoutua tai kohdata virheellistä tietoa. Laitteet eivät useinkaan voi tukeutua vain yhteen datan lähteeseen, vaan lähteen vikaantuessa tulee niiden vastaavaa dataa toisaalta. Järjestelmän tulee kyetä löytämään virheellisesti käyttäytyvät laitteet esimerkiksi niiden tuottamaa dataa analysoimalla ja tehdä sen pohjalta päätöksiä, turvaten verkon selviytymisen. (Roman ym., 2013.) Vikasietoisuuden vaatimukset sisältävät esineiden itsensä turvallisuuden, niiden ajantasaisen tietämyksen verkon tilasta ja kyvyn puolustautua vikoja ja hyökkäyksiä vastaan sekä mahdollisesta vahingosta palautumisen (Porras ym., 2018).

Koko verkon mittakaavassa tulee järjestelmän kyetä torjumaan palvelunestohyökkäyksiä. Porras ym. (2018) mainitsevat keinoälyä hyödyntävän ratkaisun, joka kykenee valvomaan laitteiden saamia pyyntöjä ja antaa palvelunestohyökkäysvaroituksen muille viereisille solmuille, jos ennakkoon päätelty maksimikapasiteetti ylitetään. Laitteet yrittävät sitten etsiä hyökkääjän IP-osoitteen perusteella ja keskeyttää pakettien vastaanottamisen tästä osoitteesta. Toisena, kustannustehokkaampana lähestymistapana he mainitsevat yksinkertaisen sink-solmun eli solmujen keräämää dataa tallentavan solmun varmuuskopioinnin.

Erityisesti esineiden Internetin eheyden turvaamiseen on esitetty lohkoketjuverkkoja. Christidisin ja Devetsikiotisin (2016) mukaan lohkoketjuja voitaisiin hyödyntää esineiden Internetissä, sillä niiden avulla solmut voisivat kommunikoida hajautetussa vertaisverkossa ilman luotettua välittäjää. Lohkoketjut mahdollistavat keskittämättömät verkot, joissa verkon osapuolien ei ole pakko luottaa toisiinsa tehokkaan samassa ketjussa tapahtuvan salauksen ansiosta. Vertaisverkot poistaisivat myös laajojen keskitettyjen IoT-verkkojen ylläpitokulut. Lohkoketjujen käyttöä rajoittaa kuitenkin keskitettyihin verkkoihin verrattuna heikko suorituskyky ja lisäksi yksityisyyden sekä luottamuksellisuuden säilyttäminen on haastavaa, sillä kaikki tapahtumat ketjussa ovat avoimia, jolloin ne ovat alttiita analysoinnille ja mahdollisesti osapuolten todellisten henkilöllisyyksien selvittämiselle. (Christidis & Devetsikiotis, 2016.)

Lohkoketjut voisivat siis sopia sovelluksiin, joissa yksityisyys ei ole erityisen tärkeää, mutta tapahtumien oikeellisuus on. Christidis ja Devetsikios (2016) mainitsevat eräänä lohkoketjuja ja esineiden Internetiä yhdistävänä kuluttajapuolen sovelluksena energiamarkkinat vertaisverkossa. Älykkäät aurinkopaneelit voisivat automaattisesti myydä ja ostaa energiaa muilta käyttäjiltä kryptovaluutalla käyttäjän asettamien kriteerien mukaan, mikä vapauttaisi ylimääräisen paneelien tuottaman energian sitä tarvitsevien käyttöön.

3.3.5 Käyttäjät, sääntely ja sovellukset

Vaikka esineiden Internet koostuukin älykkäistä laitteista, on myös niiden käyttäjät otettava huomioon turvallisuudesta puhuttaessa. Dhillonin ym. (2016) mukaan käyttäjien turvallisuustietoisuus on tärkeää IoT-ympäristöissä, koska laitteiden dataan käsiksi pääsevien käyttäjien käytös voi vaikuttaa IoT-turvallisuuteen. Turvallisuustietoisuutta voi parantaa esimerkiksi tiedottamalla käyttäjiä aktiivisesti turvallisuusuhkista, jotta nämä osaavat varautua niihin. Esineiden Internetissä tulee lisäksi edistää vastuullisen käytön kulttuuria kuluttajissa, jotta väärinkäytöksiä voidaan ehkäistä. (Dhillon ym., 2016.)

Guptan ym. (2017) mukaan käyttäjien kykenemättömyys vuorovaikutukseen järjestelmän kanssa on yksi suurimmista syistä, joka vaikuttaa ihmisten huijatuksi tulemiseen tietojenkalasteluhyökkäyksissä. Niinpä käyttäjien tietoisuudella ja kouluttamisella on merkitystä myös esineiden Internetissä tapahtuvan tietojenkalastelun kitkemisessä. Luonnollisesti tehokkainta olisi suodattaa tietojenkalasteluviestit jo ennen kuin käyttäjät pääsevät niitä näkemään. Kuten Goptan ym. (2017) tutkimuksesta käy ilmi, on tämä kuitenkin haastavaa jo perinteisessäkin Internetissä, eikä lähestymistapoja tai algoritmeja esineiden Internetiin ei ole kehitetty.

Lainsäädännöllä voidaan vaikuttaa valmistajien päätöksiin IoT-turvallisuuden alueella. Lakien tulee suojata kuluttajien datan yksityisyyttä ja rajoittaa tämän datan käyttöä. (Dhillon ym., 2016.) Aleisa ja Renaud (2017) käyttävät tähän liittyen termiä datan minimointi (*engl. data minimization*), tarkoittaen kerätyn tiedon määrän ja säilytysajan rajoittamista. Lisäksi lainsäädännössä tarvetta on eri IoT-luokkien turvallisuusstandardeille (Dhillon ym., 2016). Euroopan komissiolle tehdyn selvityksen mukaan niin kutsuttu pehmeä laki, joka sisältää standardit, valvonnan ja eettisiä piirteitä on paras ratkaisu turvallisuuden edistämiseksi samalla turvaten vapauden teollisuudelle. Yhdysvalloissa asia on ollut vasta keskustelun alla. (Porras ym., 2018.)

IoT-sovellusten turvallisuuden parantamiseksi Dhillon ym. (2016) mainitsevat käyttäjän varmemman todentamisen yhtenä konkreettisena keinona. Heidän mukaansa salasanat ovat riittämättömiä ja käyttäjän todentamisessa tulisi käyttää esimerkiksi biometrisiä tunnuksia ja kaksivaiheista todentamista. Zhaon ja Gen (2014) sekä Suon ym. (2012) mukaan sovellusten turvallisuusongelman ratkaisemiseksi tulisi hyödyntää todennusta ja avainten yhteensopivuutta läpi koko järjestelmän yksityisen tiedon suojaamisen lisäksi.

4 YHTEENVETO

Tässä kirjallisuuskatsauksena toteutetussa tutkielmassa tutkittiin esineiden Internetiä kyberturvallisuuden näkökulmasta ja kuluttajakontekstissa. Esineiden Internet on viime vuosikymmenen aikana laajentunut käsitteeksi, jonka nähdään vaikuttavan kaikkiin elämämme osa-alueisiin. Maailma, jossa kaikki esineet kommunikoivat keskenään käyttäjiltä näkymättömissä älykkäiden teknologioiden avulla mahdollistaa futuristisia sovelluksia parantaen elämänlaatua niin terveydenhuollon, älykkään elämisen ja liikenteen keinoin. Kehityksen alkumetreillä RFID- ja sensoriverkkoteknologiat nähdään keskeisinä älykkäiden esineiden luomiseksi ja verkon toteutusta vievät eteenpäin muun muassa 5G ja pilvilaskenta. Perinteinen Internet-arkkitehtuuri ei palvele esineiden Internetin tarpeita pidemmän päälle, joten nousee tarve arkkitehtuurille, joka kykenee jopa biljoonien esineiden yhdistämiseen energiatehokkaasti ja turvallisesti.

On huomattu, että nimenomaan turvallisuus on jäänyt kehityksessä takaalalle, osin valmistajien yhteistyöhaluttomuuden ja välinpitämättömyyden takia sekä myös siitä syystä, että esineiden Internetillä on huomattavasti muitakin haasteita, kuten laitteiden yhdistäminen. Nykyisissä IoT-laitteissa on selkeitä turvallisuusongelmia, mikä vähentää kuluttajien luottamusta tulevaisuuden Internetiin. Kyberturvallisuuteen on kuitenkin erityisen tärkeää kiinnittää huomiota, koska esineiden Internetin laajuus ja kaikkialla läsnäolevuus altistaa sen monimuotoisille hyökkäyksille, joiden seuraukset voivat olla katastrofaalisia. Jos esineiden Internetiin nojaudutaan yhtä vahvasti kuin on visioitu, jopa perinteisesti verrattain harmiton palvelunestohyökkäys saattaa vaarantaa ihmishenkiä. Samaan aikaan tavanomaiset riskit, kuten tietovuodot ovat yhä läsnä ja niidenkin vaikutus on vakavampi sensorien kerätessä käyttäjistä valtavia määriä entistä luottamuksellisempaa tietoa. Uhkiin on esitetty myös turvallisuustoimia niin yksittäisiä hyökkäyksiä vastaan kuin kokonaisvaltaisia esineiden Internetin turvallisuutta nostavia ratkaisuja. Tutkielmassa pyrittiin löytämään ratkaisuja esineiden Internetin turvallisuuden parantamiseen ja siten nostamaan kuluttajien luottamusta teknologiaan.

Tässä tutkimuksessa lähestymiskulma esineiden Internetin turvallisuuteen oli tunnistaa uhat ja sitten turvallisuusratkaisut. Pääasiallinen tutkimuskysymys oli: miten esineiden Internetin turvallisuuttaa voidaan parantaa? Huomattiin, että turvallisuuden parantamisessa on hyödynnettävä moninaisia eri ratkaisuja. Teknisten ratkaisujen lisäksi turvallisuutta voidaan edistää ei-teknisillä tavoilla. Lainsäädännön keinoin valmistajia voidaan pakottaa ottamaan turvallisuuskysymykset huomioon. Valmistajia voisi esimerkiksi velvoittaa päivittämään laitteitaan läpi niiden käyttöiän ja täyttämään asetetut turvallisuusvaatimukset. Euroopassa toimivia yrityksiä sitoo myös GDPR, mutta jää nähtäväksi, hidastaako sääntely esineiden Internetin kehitystä. Kehityksen tulee silti edetä turvallisuuden ja yksityisyyden ehdoilla, jotta kuluttajien luottamus voidaan säilyttää. Koska suuri osa esineiden Internetin ongelmista johtuu valmistajien siiloutumisesta, tulisi sääntelyn tähdätä sen lisäämiseen. Standardointi voisi olla tehokas keino laitteiden yhteistoimivuuden ja valmistajien yhteistyön lisäämiseen. Standardit ja yhteistyö edistäisivät esineiden Internetin arkkitehtuurin kehittämistä ottaen kaikki sovellukset ja turvallisuusvaatimukset huomioon suunnittelussa.

Luottamus ja luottamukseen perustuvat keinot vaikuttavat lupaavilta ratkaisuilta esineiden Internetiin, erityisesti todennukseen. Globaalisti toimiva luottamuspuu voisi olla päämääränä todennusongelmaa ratkaistaessa, vaikka se ei olekaan toteutettavissa vielä nykyisessä Internetissä. Koska tarve uudelle Internet-arkkitehtuurille on tunnistettu jo muutenkin, tulisi sen kehityksessä huomioida luottamuspuun integrointi ja turvallisuus muutenkin.

Kommunikoinnin turvaamiseksi on kehitettävä rajoitetulla laitteistolla toimiva, mutta tehokas salausalgoritmi ja avaintenhallintajärjestelmä. Symmetrinen salaus vaikuttaa mahdolliselta ratkaisulta tulevaisuudessa. Tulevaisuudessa teknologiset edistysaskeleet esimerkiksi akku- ja suoritinteknologiassa mahdollistavat entistä pienempiä, tehokkaampia ja virtapihimpiä laitteita, mikä mahdollistaa muun muassa vahvemman salauksen käytön. Tästä huolimatta laitteiden määrä tulee kasvamaan, joten pieni energiankulutus mahdollisimman energiatehokasta salausta hyödyntäen säilynee tavoitteena. Kuluttajien yksityisyyden turvaamiseen tulee kehittää tapoja, joilla massadataa kyetään koostamaan menettämättä sen käyttökelpoisuutta.

Lisäksi esineiden Internetin verkon on toimittava entistä älykkäämmin muun muassa haitallisten solmujen eliminoimiseksi ja palvelunestohyökkäysten estämiseksi. Tulevaisuuden tekoälyratkaisut tulevat epäilemättä olemaan keskiössä älykkäästi toimivaa verkkoa kehitettäessä. Lähettäjän ja vastaanottajan yhdistävän palvelunhallintakerroksen kehittäminen lienee avainasemassa älykkyyden lisäämisessä verkkoon.

Kuten mainittua, vastuu turvallisuudesta lankeaa osittain myös käyttäjien kontolle. Esimerkiksi tietojenkalasteluhyökkäyksiä vastaan käyttäjän valppaus on oleellista, jotta tämä osaa tunnistaa kalastelun. Parhaimmatkaan tekniset ratkaisut tuskin kykenevät torjumaan kaikkia turvallisuusuhkia. Käyttäjät voivat aiheuttaa uhkia myös toisilleen, joko hyökkääjinä tai mahdollisesti ilman aktiivista myötävaikutusta, koska käyttäjien vaarantuneet laitteet saattavat olla

hyödynnettävissä hajautetuissa kyberhyökkäyksissä. Käyttäjien turvallisuusosaamisen kehittäminen voi auttaa siis koko verkon turvallisuuden parantamisessa. Esimerkiksi turvallisuustietoisemmat käyttäjät osaisivat huolehtia salasanoistaan ja siitä, etteivät he anna tietojaan väärille tahoille. Tiivistäen esineiden Internetin turvallisuuden parantamisessa tulee hyödyntää seuraavia asioita: lainsäädäntö, standardointi, luottamus, tehokas salaus, älykkäät verkot ja käyttäjien tiedottaminen.

Tämä tutkimus käsitteli esineiden Internetin turvallisuutta varsin yleisellä tasolla, koska aihepiiri ei ole minulle kovin tuttu. Hyvän kokonaiskuvan saaminen oli aiheen paremman ymmärtämisen kannalta oleellista. Niinpä sekä turvallisuusuhkista että -ratkaisuista ei ole tässä käsitelty läheskään kaikkia. Uhkia kirjallisuudesta löytyi huomattavasti konkreettisia ratkaisuja enemmän, mikä myös nousi tutkielman rajoitteeksi.

Esineiden Internetin uutuus tarkoittaa myös sitä, että jatkotutkimusaiheita on aiheesta valtavasti. Erityisesti yksittäisten teknologioiden käyttöä turvallisuuden parantamiseen tai yksittäisten uhkien roolia esineiden Internetissä olisi aiheellista tutkia tarkemmin. Tietojenkalastelun esiintyminen ja torjuminen esineiden Internetissä on esimerkki uhkalähtöisestä aiheesta. Tietojenkalastelua esineiden Internetissä ei ole tutkittu juuri ollenkaan, vaikka se mainitaankin monesti esineiden Internetiin liittyvänä uhkana. Yksittäisistä teknologioista tarkemmin voisi tutkia lohkoketjujen käyttötapoja ja hyötyjä esineiden Internetissä ja lisäksi tehokkaita salausalgoritmeja. Lisäksi olisi aiheellista tutkia massadatan käsittelyä esineiden Internetissä ja esineiden Internetiin soveltuvia pilviratkaisuja.

LÄHTEET

Aleisa, N., & Renaud, K. (2017). Privacy of the Internet of Things: A Systematic Literature Review. *Hawaii International Conference on System Sciences 2017 (HICSS-50)*.

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 Tutorials*, 17(4), 2347–2376.

Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, 22(7), 97-114.

Atamli, A. W., & Martin, A. (2014). Threat-Based Security Analysis for the Internet of Things. *2014 International Workshop on Secure Internet of Things*, 35–43.

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

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, 58(1), 49–69.

Chahid, Y., Benabdellah, M., & Azizi, A. (2017). Internet of things security. *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, 1–6.

Chen, Y. (2012). Challenges and opportunities of internet of things. *17th Asia and South Pacific Design Automation Conference*, 383–388.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.

Covington, M. J., & Carskadden, R. (2013). Threat implications of the Internet of Things. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1–12.

Darianian, M., & Michael, M. P. (2008). Smart Home Mobile RFID-Based Internet-of-Things Systems and Services. *2008 International Conference on Advanced Computer Theory and Engineering*, 116–120.

Dhillon, G., Carter, L., & Abed, J. (2016). Defining Objectives For Securing The Internet Of Things: A Value-Focused Thinking Approach. *WISP 2016 Proceedings*.

French, A., & Shim, J. (2016). The Digital Revolution: Internet of Things, 5G, and Beyond. *Communications of the Association for Information Systems*, 38(1).

Goad, D., & Gal, U. (2017). IoT Design Challenges and the Social IoT Solution. *AMCIS 2017 Proceedings*.

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, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267.

Katagi, M., & Moriai, S. (2008). Lightweight Cryptography for the Internet of Things. *Sony Corporation*, 7-10.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *2012 10th International Conference on Frontiers of Information Technology*, 257–260.

LaBuda, R., & Gillespie, M. (2017). The Internet of Things: Current Issues and Future Problems. *SAIS 2017 Proceedings*.

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Transactions on Power Systems*, 32(4), 3317–3318.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 4(5), 1125–1142.

Liu, Z., & Zhang, M. (2018). Analysing online platform users' attitudes toward Internet of Things. *PACIS 2018 Proceedings*.

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.

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17–31.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems*, 10(26), 1-49.

Porras, J., Pänkäläinen, J., Knutas, A., & Khakurel, J. (2018). Security In The Internet Of Things - A Systematic Mapping Study. *Hawaii International Conference on System Sciences 2018 (HICSS-51)*.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266–2279.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A Review. *International Conference on Computer Science and Electronics Engineering*, IEEE, 648–651.

Tan, L., & Wang, N. (2010). Future internet: The Internet of Things. *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 5, 376-380.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23–30.

Wortmann, F., & Flüchter, K. (2015). Internet of Things - Technology and Value Added. *Business & Information Systems Engineering*, 57(3), 221–224.

Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., & Du, H.-Y. (2010). Research on the architecture of Internet of Things. *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 5, 484-487.

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.

Zhang, Z.-K., Cho, M. C. Y., & Shieh, S. (2015). Emerging Security Threats and Countermeasures in IoT. *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 1–6.

Zhao, K., & Ge, L. (2013). A Survey on the Internet of Things Security. *2013 Ninth International Conference on Computational Intelligence and Security(CIS)*, 663–667.