Olli Huuhtanen

ESINEIDEN INTERNET – NYKYAJAN JA TULEVAISUUDEN ONGELMIA SEKÄ RATKAISUJA KYBERTURVALLISUUDEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Huuhtanen, Olli
Esineiden Internet – nykyajan ja tulevaisuuden ongelmia sekä ratkaisuja kyberturvallisuuden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2017, 33 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Moilanen, Panu

Kyberturvallisuus on hyvin tärkeä osa nykyaikaista yhteiskuntaa, sillä suuri osa toiminnastamme, esimerkiksi monissa palveluissa asiointi, tapahtuu Internetin tai muun verkoston kautta. Esineiden Internet on seuraava askel digitaaliselle yhteiskunnalle, jossa perinteisten tietokoneiden lisäksi myös muutkin arkipäiväiset laitteet yhdistetään verkkoon. Esineiden Internet kuitenkin eroa perinteisestä Internetistä monessa mielessä, ja näin ollen sen myöskin sen turvallisuuden toteuttamisessa eivät kaikki perinteiset ratkaisut toimi samalla tavalla.

Tämän tutkielman tarkoituksena on käydä läpi Esineiden Internetin kyberturvallisuuden, ja jossain määrin fyysinen turvallisuuden, tilannetta tällä hetkellä. Tämä sisältää suurimpien tämän hetkisten ongelmien tarkastelua, ja siinä tapauksessa, että näihin ongelmiin on esitelty mahdollisia ratkaisuja, myös niiden esittelyä. Tutkielmassa myös tarkastellaan suppeasti Esineiden Internetin tulevaisuuden näkymiä turvallisuuden kannalta, eli mihin aiheisiin olisi tärkeää tehdä lisää tutkimusta, ja mitä tällä hetkellä tehdään turvallisuuden parantamiseksi. Tutkielman keskeisenä huomiona oli, että Esineiden Internet kohtaa monia ongelmia, jotka ovat osittain samoja kuin perinteisessä Internetissä, osittain erilaisia. Joihinkin näistä ongelmista löytyy jo ratkaisuja, mutta lisä tutkimukselle on kuitenkin paljon tarvetta käytännössä kaikilla turvallisuuden osa-alueilla, sillä ratkaisut ovat usein konseptuaalisella tasolla, johtuen siitä, että Esineiden Internetiä ei ole vielä täysin realisoitu siinä kaavassa joihin ratkaisuja olisi tarkoitus soveltaa. Kuitenkin tällä hetkellä on meneillään useita projekteja ympäri maailmaa, joiden tarkoituksena on antaa lisää tietoa Esineiden Internetin turvallisuuden takaamiseen. Suurimmaksi ongelmaksi tutkielmassa muodostui sen yleisluontoisuus, eli tutkielma ei tarkastele aihetta kovinkaan tarkasti, johtuen siitä, että se olisi kandidaatintutkielman rajoitteissa epärealistista.

Asiasanat: Esineiden Internet, IoT, kyberturvallisuus, kerrosarkkitehtuuri, hyökkäysmalleja, avainteknologiat

ABSTRACT

Huuhtanen, Olli
Internet of Things – Current day and future problems and solutions from the perspective of cyber security
Jyväskylä: University of Jyväskylä, 2017, 33 p.
Information Systems Science, Bachelor's Thesis
Supervisor: Moilanen, Panu

Cyber security is an important part of a modern society, because a large part of our daily actions, utilizing different services for example, is conducted through the Internet, or some other network. The Internet of Things is the next step for a digital society, where alongside traditional computer, other common equipment are also connected to a network. However, the Internet of Things differs from the the traditional Internet in many ways, and so not all of its security solutions are similar to those in traditional networks.

The purpose of this study is to have a look at the cyber security, and partially the physical security, of the Intenet of Things, and what is the situation at this moment. This is achieved through the presentation of some of the problems IoT is currently facing in terms of security, and the presentation of possible solutions to these problems, if they exist. The study also takes quick look at the possible future prospects of the security of the Internet of Things, meaning which areas of security should be studied more, and what is currently being done to improve security. The central finding of the study was, that the Internet of Things is facing many problems in terms of security, which are partially the same as in the tradional Internet, and partially different. Some solutions have been developed for these problems, but more research is still required, as most of these solutions exist only on a conceptual level, because the full realization of the IoT paradigm has yet to accomplished. However, there are multiple ongoing projects around the world, which plan to contribute to the security of the Internet of Things. The greatest fault of this study was in in its general nature. Because of the limitations of the scope of a Bachelor's Thesis, a deeper inspection of the subject was not feasible.

Keywords: Internet of Things, IoT, cyber security, layer architecture, attack models, key technologies

KUVIOT

SISÄLLYS

1 JOHDANTO

Teknologia kehittyy huimaa vauhtia nykymaailmassa, ja varsinkin laitteiden verkostoituminen on edennyt nopeasti viime vuosina. Tämä on antanut uusia mahdollisuuksia teknologian hyödyntämiseksi, mutta myös mahdollistanut sen pahantahtoisen hyväksikäyttämisen uusilla tavoilla.

Esineiden Internet (IoT, eng. Internet of Things) on käsite, joka on viime vuosien aikana saanut paljon huomiota. Esineiden Internetille ei ole yhtä virallista määritelmää (Mohsen & Jha, 2016), mutta yksinkertainen ja yleisesti käytetty määritelmä on, että IoT tarkoittaa arkipäiväisten esineiden liittämistä toisiinsa jonkinlaisen verkon kautta, kuten Internetin (Atrozi ym., 2010). Esimerkkinä tämän kaltaisista esineistä voidaan käyttää autoa ja sen ajotietokonetta, tai älypuhelinta. IoT –laitteiden nousuun viime vuosina on vahvasti vaikuttanut langattomien verkkojen nopea kehittyminen, joka on huomattavasti helpottanut, ja joissain tapauksissa kokonaan mahdollistanut, laitteiden yhdistämisen toisiinsa (Sicari ym., 2014). Mutta langattomat verkot ovat myös luoneet uusia mahdollisuuksia näiden laitteiden väärinkäyttöön, joka on yksi syy miksi IoT -laitteiden kehittämisessä yhtenä tärkeimpänä kysymyksenä on niiden kyberturvallisuus (Xia ym., 2012).

Turvallisuus on perinteisesti ollut erittäin tärkeä osa-alue ihmisen elämää, ja siitä lähtien kun ensimmäisiä tietokoneita ruvettiin valmistamaan ja yhdistämään toisiinsa verkon kautta, myös kyberturvallisuus on ollut tärkeä asia huomioida. Ihmiset ovat viime vuosina alkaneet huomioida kyberturvallisuuden tärkeyttä paljolti suurten tapahtumien medianhuomion takia, kuten esimerkiksi Edward Snowdenin paljastukset NSA:n tiedonkeräys toiminnasta. Esineiden Internetin nousu on kuitenkin vasta alussa, ja kuten tietokoneiden kanssa alkuvaiheessa, ihmiset eivät ole vielä kokonaan sisäistäneet sen kyberturvallisuuden tärkeyttä. Jotta IoT –laitteiden laaja leviäminen jatkuisi hyvin, turvallisuus- ja yksityisyyspalveluiden jatkuva kehittyminen tulee taata (Sicari ym., 2014).

Tutkielmani tarkoituksena on tutustua Esineiden Internetin kyberturvallisuuteen yleisellä tasolla, sillä yksittäisten laitetyyppien, kuten autojen, kyberturvallisuudesta en löytänyt tarpeeksi lähdemateriaalia. Käyn läpi kyberturvallisuuden nykyistä tasoa IoT –laitteissa ja minkälaisia kyberturvallisuus ratkaisuja

ja uhkia niissä esiintyy. Tarkastelen kyberturvallisuus ongelmia käyttäjän näkökulmasta, eli millä tavalla ne voisivat vaikuttaa IoT -laitteen käyttäjän elämään, ja kuinka niiltä voi suojautua. Esittelen tutkielmassa myös, minkälaisia teoreettisia ratkaisuja mahdollisiin ongelmiin on kehitetty, vaikka näitä ratkaisuja ei ole vielä ehditty soveltamaan käytäntöön. Lopuksi vielä kerron näiden laitteiden tulevaisuudesta ja mahdollisista kyberturvallisuus ongelmista joita voi esiintyä, ja minkälaista tutkimusta tällä hetkellä tehdään turvallisuuden edistämiseksi. Tutkielmani vastaa seuraaviin kysymyksiin:

- **Mitä ongelmia ja niiden ratkaisuja IoT –laitteiden kyberturvallisuuteen löytyy?** Tarkoituksena käydä läpi ja esitellä tärkeimpiä ongelmia ja uhkia joita IoT –laitteisiin kohdistuu tällä hetkellä, ja mitkä ovat laitteiston suurimmat heikkoudet turvallisuuden kannalta. Myöskin mahdollisia ratkaisuja näihin ongelmiin esitellään, mikäli niitä on. Tarkoitus on myös esitellä IoT:n rakennetta yleisesti, ja käydä läpi IoT:n turvallisuutta tämän rakennejaon kautta.

- **Miltä näyttää IoT –laitteiden tulevaisuus kyberturvallisuuden näkökulmasta?** Tarkoituksena tutustua erilaisiin näkökulmiin siitä, mitä IoT –laitteiden tulevaisuus näyttää varsinkin niiden kyberturvallisuuden kannalta. Onko oletettavissa niiden turvallisuuden parantuvan, vai tulevatko uhat pahenemaan? Minkälaisia potentiaalisia uhkia ja ongelmia voi muodostua tulevaisuudessa, jotka eivät välttämättä ole vielä ajankohtaisia?

Aihetta on tärkeä tutkia, sillä IoT -laitteiden liittäminen perinteiseen Internetiin johtaa useisiin turvallisuus haasteisiin, sillä nykyiset Internet- ja kommunikaatio teknologiat eivät ole suunniteltu tukemaan Esineiden Internetiä (Mohsen & Jha, 2016).

2 ESINEIDEN INTERNET – RAKENTEEN KUVAUS JA AVAINTEKNOLOGIAT

Tämän luvun tarkoituksena on esitellä mistä on kyse, kun puhutaan Esineiden Internetistä ja sen yleisemmistä rakennejaoista, sekä sen toteutuksen kannalta oleellisista avainteknologioista.

2.1 Yleinen kuvaus Esineiden Internetin rakenteesta

Loogisesta näkökulmasta katsoen, Esineiden Internet koostuu älylaitteista, jotka työskentelevät yhdessä jotain tietty tavoitetta varten, kun taas tekniseltä kannalta katsottuna IoT:ssa on kyse useista laitteista jotka hyödyntävät erilaisia kommunikaatio arkkitehtuureja, teknologia ja suunnittelu metodeja (Sicari ym., 2014). Tämä laitteiston ja teknologian heterogeenisyys voi tehdä IoT:n luokittelemisesta ja osioihin jakamisesta jokseenkin vaikeaa, mutta jotta IoT:sta saataisiin jonkinlainen järjestelmällinen käsitys, on johonkin luokitukseen ja jakoon syytä turvautua. Tässä tutkielmassa IoT:ta ja sen turvallisuutta tarkastellaan kolmiosaisen rakennejaon kannalta, sillä se on lähdemateriaalin perusteella yksi yleisimpiä tapoja jakaa IoT:n arkkitehtuuri osiin. Tätä tapaa käsitellä IoT:ta tukee myös se, että monet tutkijat jotka jakavat IoT:n eri tavalla osiin käyttävät kuitenkin joko kaikkia kolmea, tai ainakin osaa niistä, pohjana omille ehdotuksilleen.

Zhang ym. (2011) sekä Ning ym. (2013) esittelevät tämän yleisesti käytetyn kolmijaon omissa tutkielmissaan seuraavasti:

- **Havainnointikerros**, eli pohjimmainen kerros. Tässä kerroksessa sijaitsevat teknologiat ja ratkaisut joita käytetään havainnoimaan ja keräämään informaatiota fyysisestä maailmasta, esimerkkinä RFID -laitteet, jotka esitellään myöhemmin tutkielmassa.
- **Verkostokerros**, eli keskimmäinen kerros. Tätä kerrosta hyödynnetään havainnointikerroksen keräämän tiedon siirtämiseen ja prosessointiin, sekä tarjoamaan viimeiselle kerrokselle luotettavan väylän kommunikoinnille.
- Päällimmäisenä kerroksena toimii **käyttökerros**. Sen tehtävänä on käsitellä kaikki se tieto jota verkostokerros siirtää sille havainnointikerroksesta. Tässä kerroksessa hyödynnettäviä teknologioita ovat esimerkiksi pilvipalvelut ja tiedonlouhinta.

Muista arkkitehtuuri jaoista mainittakoon Chen ym. (2011), jotka lisäävät edelliseen jakoon vielä neljännen **palvelukerroksen**, jonka tarkoituksena on tuottaa erilaisia älykkäitä palveluita IoT -laitteiston käyttäjille, esimerkiksi tarkkuus

maataloutta. Toisena esimerkkinä Aazam ym. (2014) taas eivät tunnusta palvelukerrosta, vaan lisäävät arkkitehtuuri jakoon kaksi omaa kerrostaan verkostokerroksen päälle:

- **Väliohjelmistokerros,** joka vastaanottaa tietoa verkostokerrokselta, ja jonka tarkoituksena on palveluiden hallinta sekä tiedon varastointi. Se myös toteuttaa jonkin verran tiedon prosessointia ja siirtää tiedon eteenpäin käyttökerrokselle.
- **Liiketoimintakerros,** jonka tarkoituksena on tehdä liiketoimintaa ja rahaa tarjoamalla palveluita käyttäjille. Käyttökerroksessa muodostunut tieto muokataan sellaiseksi, että sitä voidaan soveltaa liiketoiminnan harjoittamiseen.

Jotkin alan tutkijat eivät taas hyödynnä ollenkaan edellisen kaltaista rakennejakoa, vaan luokittelevat Esineiden Internetin ja sen sovellukset täysin erilaisilla tavoilla, kuten jakamalla sen erilaisiin ”visioihin”, jotka sisältävät eri IoT:seen liittyviä käsitteitä (Atzori ym., 2010). Ei ole kovinkaan yllättävää, että Esineiden Internetin rakenteen jakamisesta löytyy hyvinkin eroavia mielipiteitä, sillä aihe on vielä suhteellisen nuori, eikä IoT -sovelluksia ole vielä yleisesti käytössä kaikkialla. Jotta tulevaisuudessa onnistutaan IoT -paradigman toteuttamisessa hyvin, on todennäköisesti tärkeää löytää jokin yhteinen tapa jakaa ja luokitella IoT ja sen sovellukset. Tämän hetken tutkimusmateriaalin perusteella, tässä tutkielmassa mainittu kolmijako on mahdollinen ratkaisu.

2.2 Avainteknologiat

Esineiden Internet on monimuotoinen käsite. ja siihen kuuluvat laitteet eivät ole useinkaan samanlaisia toiminnaltaan, joten myöskin niiden toteuttamiseen tarvittavat teknologiat vaihtelevat. On kuitenkin olemassa joitain avainteknologioita, joita kaikki IoT -laitteet toiminnastaan ja muodostaan riippumatta tarvitsevat, ja seuraavaksi tutkielmassa esitellään näistä tärkeimmät, sillä näiden teknologioiden tiedostaminen ja ymmärtäminen on tärkeää myös IoT:n turvallisuuden kannalta.

2.2.1 Radio Frequency IDentification (RFID) ja Near Field Communication (NFC)

RFID -laite (tai tarra/tagi) on pieni mikrosiru, joka on suunniteltu tiedon lähettämiseen langattomasti (Juels, 2006). Laite kiinnitetään usein jonkin tuotteen tai laitteen antenniin menetelmällä, joka muistuttaa tavallista liimatarraa. Mikrosiru itse voi olla erittäin pieni, jopa 0,4 mm² (Takaragi ym., 2001). Esineiden Internetissä RFID -laite usein mahdollistaa IoT -laitteen kommunikoinnin verkon kautta,

näin ollen hyödyntäen aikaisemmin esiteltyä Esineiden Internetin verkostokerrosta. Tämä kommunikointi kyky on IoT -laitteiden yksi tärkeimmistä ominaisuuksista, sillä ilman sitä laitteiden keräämä tieto ei liiku, eikä sitä siis ole mahdollista hyödyntää. RFID toimii käytännössä optisen viivakoodin tavoin tuotteen tunnistuksessa, mutta kahdella selvällä edulla siihen nähden: RFID -laite lähettää jokaiselle laitteelle ainutlaatuista sarjanumeroa, jonka avulla se erottuu lukemattomista identtisistä laitteista, ja on siis tarkempi kuin perinteinen viivakoodi tunnistuksen yhteydessä. Toisena etuna on RFID -laitteen automaattisuus, eli sen skannaus ja tunnistaminen voi tapahtua ilman näköyhteyttä skannerin ja tagin välillä. Skannaus ei myöskään vaadi samaa määrää tarkkuuttaa kuin viivakoodissa, ja RFID lukijat pystyvät lukemaan laitteita huomattavasti nopeammalla tahdilla kuin viivakoodinlukijat.

RFID -laitteiden heikkoutena voidaan mainita niiden virtalähteen tarve, jota viivakoodeilla taas ei ole. Useimmissa malleissa virta tule skannauksen yhteydessä skannerista, mutta joissain versioissa laitteessa on itsessään virtalähde, esimerkiksi pieni patteri, joka aktivoituu joko skannauksen tai tiedon lähetyksen yhteydessä. Myöskin negatiivisena huomiona RFID -laitteiden valmistuksen ja käytön hinta on suurempi kuin viivakoodien (Juels, 2006).

NFC on uudempi kommunikaatioteknologia, joka pohjautuu aikaisempaan RFID standardiin. NFC -tagien avulla IoT -laitteet voivat kommunikoida keskenään joko ollessaan kosketuksissa toisiinsa tai vähintään lähellä toisiaan, ja mahdollistaa perinteisen passiivisen tagin ja aktiivisen lukijan välisen kommunikoinnin lisäksi kahden aktiivisen lukijan välisen vertaisverkon (Want, 2011). Esimerkiksi useat älypuhelimet kommunikoivat ja vaihtavat tietoa keskenään NFC -tagien avulla (Whitmore ym., 2015).

2.2.2 Sensoriverkot

Sensoriverkot ovat myös tärkeä osa Esineiden Internetin mahdollistamista. Ne voivat toimia yhteistyössä RFID -laitteiden kanssa, parantaen näiden kykyä seurata ympäristön tilaa, kuten laitteen sijaintia tai lämpötilaa. (Atrozi ym., 2010).

Nämä verkot ovat useimmiten langattomia, ja niiden standardina toimii ZigBee protokolla (Rui ym., 2015). Itse sensorien lisäksi nämä verkot saattavat sisältää portteja, jotka keräävät tietoa sensoreista ja lähettävät sitä eteenpäin johonkin ennalta määriteltyyn serveriin. Myöskin erittäin tärkeänä osana verkkoa ovat aktuaattorit (eng. actuators), jotka toiminnallaan vaikuttavat ympäristöönsä sensorien antaman tiedon avulla. Sensorin ja aktuaattorin yhteistoiminnasta voidaan käyttää esimerkkinä palohälytintä. Hälyttimen sensori havaitsee ilmassa haitallista kaasua, ja aktuaattori laukaisee hälytyksen sensorin antaman tiedon mukaan. Tämä sensorien ja aktuaattorien yhteistoimintana on myös yksi IoT -laitteiston toiminnan tärkeimmistä tavoitteista (Whitmore ym., 2015).

2.2.3 Pilvipalvelut

Pilvipalvelut ovat lopputulos perinteisen tietokoneteknologian ja verkkoteknologian yhdistämisestä, joka syntyi suurien tietomäärien käsittelyn tarpeesta (Rui

ym., 2015). Nykyisin pilvipalveluita tarjotaan käyttäjille neljässä eri muodossa (Aazam ym., 2014): **Software as a Service (SaaS),** jossa käyttäjä hyödyntää sovelluksia verkon kautta, **Platform as a Service (PaaS)**, jossa käyttäjälle tarjotaan verkon kautta alusta jolle rakentaa sovelluksia ja palveluita. **Networks as a Service (NaaS)** taas tarjoaa käyttäjälle halutun määrän virtuaaliverkkoja, joille tämä voi määrittää omat toimintaperiaatteensa, sekä viimeisenä **Infrastructure as a Service (IaaS)** antaa käyttäjälle mahdollisuuden hyödyntää laskenta- ja tallennuspalveluita verkon kautta omien fyysisten laitteiden käytön sijaan.

Kiitos Esineiden Internetin, tiedonmäärä verkostoissa on kasvanut suuresti, ja kasvu tulee todennäköisesti jatkumaan, sillä verkkoon yhdistettyjen laitteiden määrä lisääntyy koko ajan. Tämä taas tekee pilvipalveluista välttämättömiä perinteisten fyysisten tiedontallennus menetelmien osoittautuessa riittämättömiksi. Tätä IoT:n ja pilvipalveluiden yhdistymää kutsutaan myös nimellä Esineiden Pilvi (CoT, eng. Cloud of Things) (Aazam ym. 2014). Esineiden Internetin riippuvuus pilvipalveluista on myös yksi avaintekijöistä sen kyberturvallisuudesta puhuttaessa, koska tällöin pelkästään IoT -laitteidein turvallisuus ei riitä, vaan myös niiden keräämän ja lähettämän tiedon varastona toimivan pilvipalvelun tulee olla suojattu.

Nämä kolme teknologiaa muodostavat Esineiden Internetin toiminnan perustan, ja ilman jokaista osiota IoT:n toteuttaminen nykyisellä tavalla on joko mahdotonta, tai ainakin hyvin vaikeaa. Lähdemateriaalin perusteella suurin osa aiheen tutkijoista, kuten Atzori ym. (2010); Dlamini ym. (2009); Weber (2010) sekä Zhang ym. (2011) pitävät näistä teknologioista tärkeimpänä RFID ja NFC laitteita, sillä ne toimivat IoT:n kommunikaation perustana. Pilvipalvelut ja sensoriverkot mahdollistavat IoT:n tiedon keräämisen ja tallentamisen, mutta ne ovat hyödyttömiä, jos IoT -laitteistolla ei olisi kykyä välittää tietoa eteenpäin.

Seuraavassa tutkielman osiossa käydään läpi joitain käytännön sovelluksia, joita IoT -laitteistolle löytyy tällä hetkellä. Luonnollisesti tutkielman rajoitteista johtuen kaikkia mahdollisia sovelluksia ei voida tarkastella, ja niiden esimerkki sovellusten kohdalta jotka mainitaan, on kyseessä vain pintaraapaisu. Tämä johtuu siitä, että vaikka tutkielmalle tärkeää on selventää IoT:n rakennetta ja sen sovelluksia, näiden turvallisuuden läpikäyminen on kuitenkin päätarkoituksena.

2.3 Käytännön sovelluksia

Vaikka Esineiden Internetistä puhutaan vielä jossain määrin tulevaisuuden visiona, sillä on kuitenkin jo nykyään monia käytännön sovelluksia. Chen ym. (2014) listaavat näistä joitain:

- **Laitteen sijainnin havainnointi sekä ilmoittaminen**. IoT -laite pystyy oman sijaintinsa perusteella tarjoamaan käyttäjälle tälle sijainnille kohdennettuja palveluja. Näitä palveluita voivat esimerkiksi olla jonkin tuotteen tilan valvonta tai liikenteen uudelleen ohjaus ruuhkatietojen perusteella.

- **Ympäristön havainnointi**. IoT -laite pystyy keräämään ja käsittelemään ympäristöään koskevaa fyysistä ja kemiallista tietoa, esimerkiksi lämpötilasta ja ilmankosteudesta. Näitä ominaisuuksia hyödynnetään tyypillisesti ympäristön muutosten havainnoinnissa ja lääketieteellisessä etävalvonnassa.
- **Etähallinta.** IoT -järjestelmät pystyvät hallitsemaan päätelaitteita ja toteuttamaan komentoja laitteiden keräämän informaation perusteella. Tästä esimerkkeinä voidaan pitää laitehallintaa ja katastrofeista elpymistä.
- **Turvallinen kommunikointi.** Järjestelmä voi perustaa turvallisen tiedonvälitys kanavan sovelluksen tai palvelualustan ja IoT -päätteen välille, riippuen palvelun vaatimuksista.

Tulevaisuuden potentiaalisista sovelluksista he mainitsevat **Ad hoc -verkostoitumisen**, eli IoT:lla tulisi olla nopeasti itseorganisoituvat verkostointi kyvyt sekä kyky yhteistoimia verkosto- ja palvelukerrosten kanssa tarjotakseen kyseisiä palveluja.

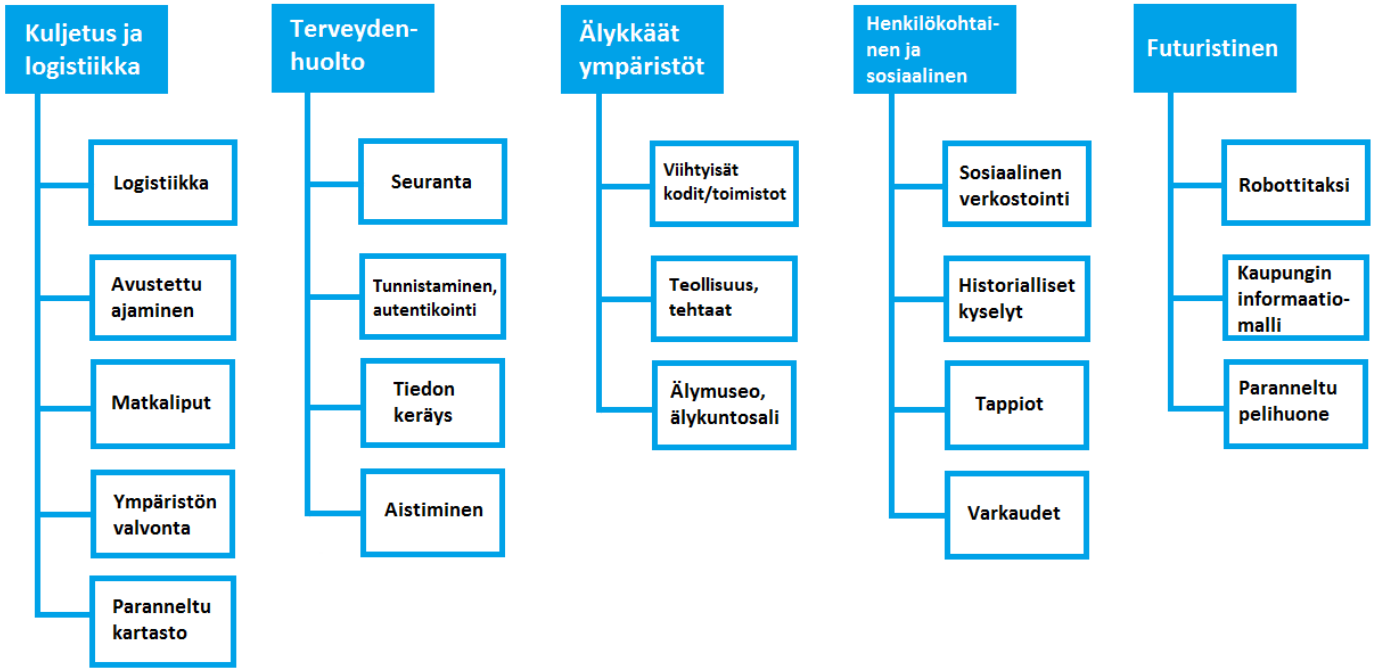
Chen ym. myös listaavat **älykaupungit** esimerkkinä laajemman mittakaavan IoT -sovelluksesta**.** Nam & Pardo (2011) määrittelevät älykaupungin olevan kaupunki jolla on huomattava omistautuminen innovaatioihin teknologiassa, hallinnassa ja toimintaperiaatteissa. Älykaupunkien teknologia osuus muodostuu paljolti IoT:sta, joka näkyy lähes kaikkialla sen palveluissa ja infrastruktuurissa, kuten liikenteen ja sään valvonnassa (Elmaghraby & Losavio, 2014). Caragliu ym. (2011) antavat esimerkkeinä nykyajan älykaupungeista Frankfurtin. Tosin on tärkeää huomata, että Frankfurt ja monet muut kaupungit jotka Caragliu ym. mainitsevat täyttävät älykaupunkien vaatimukset vain osittain. Tällä hetkellä ei löydy kaupunkia joka täyttäisi kaikki nämä vaatimukset, vaan se on paljolti visio tulevaisuudesta.

Mohsen & Jha (2016) myöskin listaavat erilaisia käytännön sovelluksia Esineiden Internetille, joista Chen ym. eivät puhuneet tai mainitsivat vain ohimennen omassa tutkimuksessaan. Ensimmäisenä esimerkkinä Mohsen & Jha mainitsevat **älyajoneuvot**, jotka voidaan esimerkiksi avata ja lukita etänä, pystyvät lataamaan verkosta tiekarttoja sekä pääsevät käsiksi liikenne tietoihin langattomasti. Myöskin **energiankulutuksesta ja hallinnasta** löytyy mahdollisia sovelluksia, esimerkiksi käyttäjät voivat hallita etänä kodin sähkölaitteita niiden antamien tietojen mukaan, kuten perustamalla jonkinlaisen aikataulun laitteiden käynnistymiseen ja päälläolemiseen energian säästämiseksi.

IoT -sovelluksia löytyy käytännössä melkein kaikista mahdollisista nykyyhteiskunnan osa-alueista, ja seuraavassa kuviossa näemme miten Atzori ym. (2010) listaavat näitä sovelluksia hyvinkin laajalti, ja miten he jakavat nämä sovellukset eri kategorioihin usealla eri yhteiskunnan tasolla. Kuten kuvio hyvin selventää, IoT -sovelluksia on käytännössä niin paljon, että niiden kaikkien listaaminen ja selventäminen ei ole käytännössä järkevää tämän tutkielman puitteissa, sillä paino pisteen tulisi olla turvallisuuden puolella. Kuitenkin vielä huomiona IoT:n sovelluksista voidaan painottaa älykaupunkien tärkeyttä. Kaikki so-

vellukset, joita Atzori ym., Chen ym., ja Mohsen & Jha mainitsivat, voidaan hyödyntää älykaupungeissa, joissa IoT -teknologian on tarkoitus ilmentyä kaikissa kaupungin toiminnoissa ja palveluissa.

Tutkielmassa on nyt esitelty Esineiden Internetin yleisimmät piirteet sekä käytännön sovellukset, ja seuraavaksi siirrytään tutkielman pääaiheeseen, eli IoT:n turvallisuuteen. Tämä turvallisuuden tarkastelu tapahtuu tähän mennessä esiteltyjen IoT:n rakenteiden, piirteiden ja sovellusten pohjalta, joka on pääsyynä niiden esittelyyn tutkielman aikaisemmissa osioissa.



KUVIO 1 IoT -sovellusten alat ja tärkeät skenaariot (Atrozi ym., 2010)

3 KYBERTURVALLISUUS, HAASTEITA JA RATKAISUJA

Edellisessä luvussa esitellyt yleisimmät arkkitehtuuri jaot sekä avainteknologiat herättävät huomattavan määrän kyberturvallisuus kysymyksiä, sillä vaikka monet IoT:n turvallisuusratkaisut pohjautuvat perinteistä Internetiä varten kehitettyihin ratkaisuihin, IoT:n suuri skaalautuvuus (Zhang, B., ym., 2011) sekä laitteiston heterogeenisyys verrattuna perinteiseen Internettiin vaativat näiden ratkaisujen mukauttamista (Zhang, Z., ym., 2015). IoT -laitteiston mahdollinen julkinen sijainti (kuten katuvalojet ja niiden sensorit) on myös yksi potentiaalinen uhkatekijä (Roman ym., 2011) jota ei esiinny muissa verkoissa. Kuitenkin perinteisen kyberturvallisuuden toteutus periaatteet, kuten uhkien estäminen ennen niiden tapahtumista, pätevät myös IoT:sta puhuttaessa.

Seuraavaksi tutkielmassa keskitytään siihen, miten Esineiden Internetin omat arkkitehtuuri ratkaisut vaikuttavat sen kyberturvallisuuteen, ja miten perinteisten verkkojen turvallisuuskonseptit (kuten yksityisyys ja luottamus) näkyvät IoT:ssa. Näiden jälkeen myös käsitellään mahdollisia hyökkäysvektoreita ja syitä siihen, miksi joku haluaisi hyökätä IoT -verkkoa tai -laitetta vastaan.

3.1 Kerrosarkkitehtuurin turvallisuus

Aiemmin tutkielmassa käytiin läpi yleisimpiä tapoja, joilla IoT arkkitehtuuri jaetaan erilaisiin kerroksiin. Tässä luvussa tarkastellaan miten IoT:n kyberturvallisuus (ja jossain määrin fyysinen turvallisuus) voidaan käsitellä näissä kerroksissa. Koska yleisin kerrosjako oli havainnointikerros, verkostokerros sekä käyttökerros, tämän luvun katsaus turvallisuuteen tapahtuu tästä näkökulmasta katsoen.

3.1.1 Havainnointikerros

Havainnointikerroksen laitteisto sijaitsee IoT verkoston laidoilla, ja niillä on usein hyvinkin rajattu laskenta-, varastointi- ja kommunikointi kapasiteetti (Chen ym., 2011). Nämä laitteet saattavat usein myös fyysisesti sijaita ympäristössä jossa niiden valvonta on haasteellista, altistaen ne muillekin kuin kyberhyökkäyksille (Zhang ym., 2011). Näistä syistä johtuen monet perinteiset turvallisuusratkaisut eivät toimi suoraan näissä laitteissa ilman soveltamista esiteltyihin rajoituksiin, ja tämä soveltaminen vuorostaan heikentäisi näiden ratkaisujen toimivuutta.

Yhtenä ratkaisuna havainnointikerroksen turvallisuus ongelmiin Chen ym. ja Zhang ym. ehdottavat kevyen salaus- ja avaintenhallinta protokollan (eng. a lightweight key management protocol) kehittämistä, jonka toimintaa laitteiden rajoitettu suoristusteho ei haittaisi. Mohsen & Jha (2016) kertovat että laitteiden mikropiirien muokkaus on yksi tehokkaimpia suojautumiskeinoja fyysisiä uhkia

vastaan. Esimerkiksi voitaisiin hyödyntää nykyisissä palohälyttimissä esiintyvää peukaloinnin estoa muistuttavaa ratkaisua. Äärimmäisissä tapauksissa laitteistoon voidaan asentaa itsetuho ominaisuus, joka tekee laitteesta käyttökelvottoman sen vaarannuttua. Mohsen & Jha mainitsevat myös näiden laitteiden mahdolliset informaation vuodot turvallisuusongelmana. Näitä vuotoja voitaisiin minimoida käyttämällä esimerkiksi satunnaistetulla viiveellä tai tarkoituksella tuotetulla ”taustaäänellä”, jonka on tarkoitus hämätä muita laitteita jotka mahdollisesti yrittävät päästä käsiksi IoT -laitteen lähettämiin tietoihin.

3.1.2 Verkostokerros

Puhuessaan verkostokerroksen turvallisuudesta Zhang ym. (2011) jakavat kerroksen kahteen tyyppiin pääsykerroksen ja ydinkerroksen lähetysten mukaan. Pääsykerroksessa suurin turvallisuusongelma muodostuu heterogeenisyydestä, johtuen erilaisista käytetyistä teknologioista laitteen paikannuksessa ja kommunikoinnissa, jotka vaihtelevat laitteesta toiseen. Myöskin laitteiston langaton kommunikointi muodostaa mahdollisen ongelman, sillä nämä verkot ovat kohtuullisen avoimia, ja näin ollen antavat mahdollisille hyökkääjille tilaisuuden muokata ja sabotoida laitteiston lähettämiä viestejä oman mielensä mukaan. Ydinkerros taas pystyy hyödyntämään perinteisiä verkkoturvallisuuden ratkaisuja, mutta joutuu tästä syystä myös painimaan monien perinteisten verkkojen turvallisuusuhkien kanssa, jotka eivät taas vaikuta pääsykerrokseen. Chen ym. (2014) myöskin huomauttavat, että verkostokerrokselle aiheutuu ongelmia turvallisuuden suhteen ei pelkästään laitteiston ja teknologioiden, vaan myös itse verkkojen heterogeenisyyden vuoksi.

Mohsen & Jha (2016) listaavat joitain ratkaisuja verkostokerroksen ja IoT:n kommunikoinnin turvallisuuteen. Ensimmäisenä he mainitsevat luotettavat reitityksen rakentamisen tärkeyden. Heidän mukaansa IoT:ssa jotkin välittäjät ja serverit saattavat vaatia suoraa pääsyä viestin sisältöön ennen kuin lähettävät sen eteenpäin. Tästä johtuen potentiaaliset hyökkääjät saattavat päästä kiinni näiden viestien tietoihin hyödyntäen tätä vaatimusta, jos reititys ei ole tarpeeksi luotettava. Toinen ratkaisu, joka on heidän mukaansa välttämätön, on IDS:n (eng. Intrusion Detection System) käyttäminen valvomaan verkkotapahtumia ja kommunikaatio yhteyksiä. IDS nostaisi hälytyksen, jos se havaitsisi poikkeavaa toimintaa valvontansa alla olevissa verkoissa ja yhteyksissä. Perinteisesti IDS:n toiminta on keskittynyt Internettiin, mutta viime aikoina myös IoT:lle tehtyjä versiota on alkanut ilmestyä.

Ozturk ym. (2004) ehdottavat tulvinta perusteista liikenteenvastaista analyysi mekanismia (eng. flooding based anti-traffic analysis mechanism), jonka tarkoituksena olisi estää verkoston ulkoista hyökkääjää paikantamasta tiedonlähteen sijaintia. Heidän mukaansa tulvintaa on kolme lähestymistapaa: lähtökohtainen, jossa jokainen solmu verkossa välittää tietopakettia eteenpäin vain kerran, todennäköisyyspohjainen, jossa vain osa verkoston kaikista solmuista välittää tietoa eteenpäin ja loput hylkäävät saamansa viestit, ja kolmantena haamupohjainen, jossa lähden lähettää viestinsä satunnaisella tavalla, jonka jälkeen viestiin käytetään lähtökohtaista tulvintaa (eng. baseline flooding).

3.1.3 Käyttökerros

Käyttökerroksen suurimmiksi ongelmiksi Zhang ym. (2011) listaavat suuren vaihtelevaisuuden laitteiston välillä sekä käyttäjien yksityisyyden turvaaminen. Käyttökerroksen laitteisto on useimmiten käyttäjien hyödyntämää päätelaitteistoa, joten suuri variaatio laitteiden välillä on hyvin ymmärrettävää, ja sen välttäminen tuskin tulee olemaan mahdollista, sillä IoT -laitteille on useita valmistusperiaatteita, laitevalmistajia sekä käyttötarkoituksia. Käyttäjien yksityisyys taas aiheuttaa ongelmia, sillä turvallisuus järjestelmien tulisi estää vieraiden tahojen pääsy yksityisiin tietoihin, mutta samalla antaa käyttäjälle mahdollisuus nähdä ja hallita näitä tietoja. Chen ym. (2014) ovat paljolti samaa mieltä käyttökerroksen turvallisuusongelmista kuin Zhang ym. He kuitenkin huomauttavat, että usein useat IoT -päätelaitteet käyttävät samaa havainnointi- ja verkostokerroksen antamaa tietoa, mutta kuitenkin vaativat erilaista tarkkuutta tältä samalta tiedolta. Tämä on ongelma, sillä jos tarjotun tiedon tarkkuus määritellään kaikkein vaativimpien laitteiden kriteerien mukaan, joillekin laitteille tarjotaan tällöin liiankin tarkkaa tietoa jolle niillä ei ole käyttöä, mutta joka kuitenkin vaatii ylimääräisiä turvallisuus toimia yksityisyyden turvaamiseksi. Ja koska IoT -laitteistolla on useimmiten rajatusti resursseja käytössä turvallisuusjärjestelmien käyttämiseen, tämä muodostaa ongelman. Jing ym. (2014) mukaan taas käyttökerroksen suurin turvallisuus ongelma muodostuu pilvipalveluiden hyödyntämisestä. Tämä johtuu siitä, että pilvipalvelut kryptaavat ja varmuuskopioivat käyttäjiensä tiedot, eivätkä poista niitä heti käyttäjän poistaessa tietonsa palvelusta. Myöskin monet yrityksen nykyään varastoivat tietojansa pilveen, tehden niistä houkuttelevia kohteita tietomurroille. Varsinkin julkisiin pilvipalveluihin varastoidut tiedot ovat vaarassa, sillä näihin palveluihin pahantahtoiset osapuolet pääsevät helpoiten käsiksi.

Jokaiselle Esineiden Internetin kerrokselle kohdistuu omanlaisia ongelmia turvallisuuden takaamisen kannalta, mutta monet näistä ongelmista voidaan lukea johtuvan samoista IoT -laitteiston ominaisuuksista, kerroksesta riippumatta. Lähes kaikki tutkielmassa hyödynnetty lähdemateriaali yhtyy samoihin johtopäätöksiin IoT -arkkitehtuurin suurimmista ongelmista turvallisuuden suhteen: rajatut resurssit joita laitteisto voi hyödyntää turvallisuusratkaisujen toteuttamiseen, sekä tämän saman laitteiston heterogeenisyys. Lisäksi Chen ym. myöskin mainitsevat IoT:n aiheuttavat ongelmia perinteisen jaetun tietokantateknologian suhteen, johtuen suurista datan reaaliaikaisista varastointi ja kysely vaatimuksista.

Seuraavassa tutkielman osiossa tarkastellaan IoT:n turvallisuutta erilaisten konseptien ja osa-alueiden kannalta, jotka ovat tällä hetkellä tärkeässä roolissa perinteisen Internetissä ja muissa vastaavissa verkoissa. Tarkoituksena on selventää kuinka nämä konseptit sekä osa-alueet sopivat Esineiden Internettiin, ja toimivatko perinteiset ratkaisut myös tässä uudessa ympäristössä, vai onko tarvetta uusien ratkaisujen kehittämiseen.

3.2 Turvallisuuden konsepteja ja osa-alueita

Esineiden Internetin turvallisuus voidaan jakaa paljolti samalla tavalla osa-alueisiin kuin perinteinenkin kyberturvallisuus, joillain lisäyksillä tosin. Selviä eroja kuitenkin löytyy turvallisuusratkaisuista ja niiden toteutuksista näillä osa-alueilla. Tässä tutkielman osiossa käydään läpi kyberturvallisuuden eri osa-alueita ja konsepteja, ja kuinka niiden ongelmia on yritetty ja yritetään ratkaista IoT -ympäristössä.

3.2.1 Yksityisyys, tiedon keräys ja säilytys

Roman ym. (2011) pitävät yksityisyyttä ja tiedon turvallisuutta hyvinkin tärkeänä osa-alueena IoT:ssa. Tiedon räjähdysmäinen kasvu on lisännyt käyttäjien valvontaa ja seurantaa Internetissä, ja IoT tulee kasvattamaan tästä syntyviä turvallisuusongelmia sen valtavasta data määrästä johtuen. He ehdottavat tähän ongelmaan ensimmäisenä ratkaisuna käyttäjille tarjottuja työkaluja omien tietojensa yksityisyyden hallintaan. Toisena ratkaisuna heidän mukaansa tiedon keräämisestä voidaan tehdä läpinäkyvää, joka tarkoittaa sitä, että käyttäjät voivat olla halutessaan tietoisia mitä tietoa heistä kerätään, sekä miten ja milloin sitä kerätään. Viimeisenä he ehdottavat yleisten rajoitteiden asettamisen sille, miten, mitä ja kuinka paljon tietoa voidaan kerätä laitteiden käyttäjiltä.

Atzori ym. (2010) esittävät myös omia näkemyksiään turvallisuus ongelmista ja ratkaisuista yksityisyyden ja tiedon säilyttämisen suhteen. Heillä on siinä mielessä erilainen näkemys Roman ym. verrattuna, että heidän mukaansa ei ole mahdollista antaa käyttäjille kaikkia tarvittavia työkaluja heidän omien tietojensa salausta varten, sillä IoT:n tiedonhankinta ja -hallinta keinot eroavat huomattavasti perinteisen Internetin keinoista, ja ihmisten henkilökohtaisia tietoja kerätään todella suuria määriä, tehden näiden tietojen salauksesta ja suojauksesta hyvin vaikeaa. Myöskin tiedon tallentaminen on muuttumassa yhä halvemmaksi, joka mahdollistaa yksilöiden tietojen säilyttämisen hyvinkin pitkiä aikoja. He kuitenkin ovat siitä samaa mieltä Roman ym. kanssa että edes jonkinlaisia rajoitteita tulisi asettaa tiedon keräämiselle yksityisyyden takaamiseksi, joko käyttäjän toimesta tai puolueettoman tahon puolesta. He myöskin mainitsevat, että vaikka tietoa voidaan periaatteessa säilyttää lähes ikuisesti tarvittaessa, tätäkin tulisi rajoittaa vain sille aikavälille, kun tietoa ehdottomasti tarvitaan. Whitmore ym. (2015) ehdottavat että tiedon lukija/kerääjä ja laite voisivat tarkistaa toistensa yksityisyys käytännöt ennen tiedon keräystä, varmistaakseen lukijan oikeudet päästä käsiksi näihin tietoihin.

Rodrigo ym. (2013) huomauttavat että yleisesti määritellyt rajoitteet tiedon keräämiselle eivät kuitenkaan ole varma keino estää ylimääräisen tiedon keräämistä käyttäjiltä, sillä moni taho tekee tätä laittomasti ja lupaa kysymättä. Ratkaisuina yksityisyyden hallintaan he painottavat ihmisen roolia ehdottamalla panostusta laitteiden käyttöliittymän kehittämiseen, jotta vahingot ja väärinymmärrykset laitteiden käyttämisessä vähentyisivät. Laittomaan tiedon keräämiseen he ehdottavat turvallisuus järjestelmää joka pitäisi käyttäjän ympäristöä

operatiivisena järjestelmänä, näin ollen skannaten kaiken tiedon joka tulee sisään tai siirtyy ulos. Heidän mukaansa myöskin käyttäjien tietoisuutta ympäristöstään tulisi kasvattaa, jotta he osaisivat olla varovaisempia.

Sicari ym. (2014) kertovat että tällä hetkellä IoT:n yksityisyyden turvaaminen ei ole kattavasti toteutettu, ja näin ollen on vielä paljon tilaa aiheen tutkimiselle. Esimerkiksi yksityisyys käytännöt eivät ole hyvin määriteltyjä tai yhtenäisiä, ja myöskin IoT:lle ominaiset suuri skaalautuvuus ja dynaaminen ympäristö aiheuttavat ongelmia myös yksityisyyden kannalta. Tähän johtopäätökseen voidaan myös saapua muiden lähdemateriaalien perusteella, sillä Atzori ym., Rodrigo ym., Roman ym. sekä Whitmore ym. eivät esittele ratkaisuja kaikkiin mainittuihin IoT:n ongelmiin yksityisyyden, tiedon keräyksen sekä säilytyksen kannalta.

3.2.2 Identiteettien hallinta, luottamus ja luottamuksellisuus

Esineiden Internetissä uniikin identiteetin omaavia laitteita on huomattavasti suurempi määrä kuin perinteisessä Internetissä, ja tämä määrä tulee vielä todennäköisesti kasvamaan huomattavasti, sillä laitteiden erottaminen toiminnaltaan samankaltaisista laitteista on tärkeää myös kyberturvallisuuden kannalta. Identiteettien hallinnasta puhuttaessa Roman ym. (2011) määrittelevät neljä periaatetta joita IoT -laitteiden tulisi noudattaa:

- Esineen identiteetti ei ole sama asia kuin sen toimintalaitteiston identiteetti. Esimerkiksi röntgenlaitteella voi olla IP-osoite, mutta sillä tulisi olla myös oma identiteetti jolla se erottuu muista laitteista.
- Esineellä saattaa olla ydinidentiteetin lisäksi useita väliaikaisia identiteettejä, jotka muuttuvat esineen kulloisenkin tehtävän mukaan. Esimerkiksi sairaalalla on aina sama ydinidentiteetti, ja väliaikainen saattaisi olla esimerkiksi suojana toimiminen.
- Esine voi tunnistaa itsensä identiteetin tai sen jonkin tietyn ominaisuuden avulla. Esimerkiksi ruuan virtuaali-identiteetti perustuu sen ainesosiin ja määrään.
- Esineet tunnistavat omistajansa identiteetin. Esimerkiksi jos laite seuraa omistajansa jonkin terveyteen liittyvän ominaisuuden tilaa, sen pitäisi osata tulkita tätä tilaa suhteessa muihin omistajansa terveydellisiin ominaisuuksiin.

Heidän mukaansa lupaava lähestymistapa identiteettien hallinnan ongelmien ratkaisemiseen on useiden erilaisten ihmisten ja laitteiden todennusjärjestelmien yhdistäminen. Esimerkiksi sisäänpääsy jonnekin turvatulle alueelle voisi olla yhdistetyn sormenjälki ja henkilökortin skannerin takana.

Zhang ym. (2015) myöskin yhtyvät samaan ajatukseen, että identiteettien hallinta on vaikeaa IoT -ympäristössä sen heterogeenisyyden vuoksi. He tosin eivät mainitse Roman ym. esittelemää neljää periaatetta joita IoT -laitteiston tulisi noudattaa. Heidän mukaansa perinteisen Internetin nimeämiskeinot eivät riitä

IoT:lle, vaan uusia ratkaisuja vaaditaan. He mainitsevat yhtenä mahdollisena nimeämisperiaatteena NDN:än (Named Data Network), jossa verkkoarkkitehtuuri on isäntäkeskeisen sijaan tietokeskeinen. NDN:än mukaan nimeäminen tapahtuu IP-osoitteen sijaan laitteen varsinaisen nimen mukaan. NDN on kuitenkin vielä alkutekijöissä, ja ongelmia on esimerkiksi sen tehokkuudessa ja laitteiden todennuksessa.

Luottamus on Roman ym. (2011) mukaan elintärkeää IoT:lle, jonka kontekstissa se tarkoittaa mekanismia jolla mitataan laitteiden välisen kanssa käymisen epävarmuutta. Se voi kuitenkin myös edustaa perinteisempää tarkoitusta, eli miltä käyttäjältä tuntuu toimia IoT -ympäristössä. Tämän edistämiseen heidän mukaansa auttaa hallintakyky. Jos käyttäjälle annetaan työkaluja joiden avulla hän voi hallita omia laitteitaan ja ympäristöään, tämä todennäköisesti lisää käyttäjän luottamusta IoT:hen. Myöskin jonkinlainen hallinta palveluntarjoajan puolelta on suotavaa hyvän luottamuksen luomiseksi, kuitenkin liika hallinta voi johtaa holhoavaan ympäristöön jossa käyttäjällä ei ole tarpeeksi valtaa päättää omista asioistaan (Rodrigo ym., 2013). Ratkaisuksi luottamuksen muodostamiin ongelmiin Rodrigo ym. ehdottavat IoT:n osioiden analysointia, ja miten kukin näistä osioista (esim. verkostot) toimivat keskenään luottamuksen luomiseksi. Tämän analyysin pohjalta voitaisiin kehittää järjestelmiä luottamuksen parantamiseksi laitteiston välillä. Tämä tapa ei kuitenkaan huomioi ihmisen ja laitteen välistä luottamusta. Siihen Rodrigo ym. ehdottavat esimerkiksi käyttäjien ylläpitämää luottamuspiiriä, jossa käyttäjät arvioivat toistensa luotettavuutta.

Ratkaisemattomia ongelmia luotettavuudessa IoT -ympäristössä on vielä useita. Sicari ym. (2014) listaavat näistä hyvin määritetyn luottamuksen neuvottelukielen löytämisen, joka tukisi IoT:n yhteen toimivuutta, kunnollisen objektien identiteetin hallintajärjestelmän, sekä luottamuksen neuvottelu mekanismien kehittämiseen, jonka tarkoituksena olisi käsitellä tietovirran pääsyn hallintaa.

Identiteettien hallinnan, luottamuksen ja luottamuksellisuuden ongelmista puhuttaessa suurin osa käytetystä lähdemateriaalista on samaa mieltä, vaikka esitellyt ratkaisut eroavatkin toisistaan jossain määrin. Yhteneviä mielipiteitä esiintyy kuitenkin esimerkiksi Rodrigo ja muilla sekä Roman ja muilla. kesken laitteiston hallintakyvyn tärkeyden suhteen, vaikka heillä onkin eroavia mielipiteitä tämän hallinnan määrästä, jota laitteiden käyttäjälle tulisi antaa. Kaikki kuitenkin pitävät näitä konsepteja elintärkeinä IoT:n onnistumista varten.

3.2.3 Vikasieto

IoT:ssa tulee sen rakenteesta huolimatta olemaan miljardeja olioita, jotka toimivat tiedon välittäjinä (Roman ym., 2011). Tästä syystä laitteiden viansieto on tärkeä ominaisuus, sillä on oletettavaa, että iso osa näistä laitteista tulee kärsimään ongelmista ajoittain, johtuen esimerkiksi virheellisestä tiedosta. Roman ym. mukaansa tässä tilanteessa IoT -laitteella tulee olla kyky etsiä toinen tietolähde, joka pystyy tarjoamaan vastaavaa tietoa. Myöskin Rodrigo ym. (2013) pitävät viansietoa tärkeänä paljolti samoista syistä, mutta myös huomattavat IoT -laitteiden

rajoitetut resurssit yhtenä syynä vikojen ilmaantumiseen. Heidän mukaansa vikasiedon saavuttaminen vaatii kolmea yhteistoiminnallista asiaa:

- Ensiksi, kaikkien laitteiden tulee olla turvallisia oletuksena, sillä ei ole toteuttamiskelpoista päivittää miljardeja laitteita jälkikäteen turvallisiksi.
- Toiseksi, kaikille IoT -laitteille pitäisi antaa kyky nähdä kytketyn verkon ja sen palveluiden tila.
- Kolmanneksi, laitteiden tulisi kyetä puolustaa itseään verkkojen kaatumista ja hyökkäyksiä vastaan. Kaikissa laitteissa tulisi olla mekanismit jotka mahdollistaisivat vastatoimien käynnistämisen, esimerkiksi laitteen sammuttamisen, epätavallisessa tilanteessa.

Esineiden Internetillä on turvallisuuden kannalta ongelmia käytännössä jokaisella osa-alueella, joita esiintyy perinteisessä Internetissä ja muissa vastaavan kaltaisissa verkostoissa. Tässä tutkielman osiossa näistä esiteltiin lähdemateriaalin perusteella vain huomattavimmat, sillä kaikkien konseptien läpikäyminen olisi tämän tutkielman rajoitteiden puitteissa epäkäytännöllistä.

3.3 Hyökkäysmalleja ja -motivaatiotekijöitä

Jokaiseen kerrokseen, johon Esineiden Internet on yleisesti jaettu, kohdistuu erilaisia uhkia. Ne saattavat keskittyä vain joihinkin tiettyihin laitetyyppeihin, tai mahdollisesti olla uhka kaikille saman kerroksen laitteille tai koko IoT:n laitteistolle kerroksesta riippumatta. Turvallisuuden toteuttamisen ja suunnittelun kannalta näiden uhkatekijöiden tunteminen on elintärkeää. Abomhara & Kien (2015) jakavat ihmisten aiheuttamat uhat kahteen osaan: sisäiseen, eli hyökkääjää on valtuutettu pääsemään järjestelmään sisään, ja ulkoiseen, jossa hyökkääjä toimii verkon ulkopuolelta. Nämä sisäiset ja ulkoiset uhat voidaan heidän mukaansa kategorisoida kahdelle tavalla: Epästrukturoidut hyökkäykset, jotka usein ovat kokemattomien hyökkääjien aiheuttamia, käyttäen helposti saatavia työkaluja, sekä strukturoidut hyökkäykset, jossa hyökkääjät tuntevat järjestelmän ja sen toiminnan, ja voivat hyödyntää sen heikkouksia.

Seuraavassa tutkielman osiossa käydään läpi mitä varsinaisia hyökkäysmalleja IoT:lle löytyy, miten ja minne ne vaikuttavat, sekä mitä mahdollisia syitä hyökkääjillä voi olla hyökätä IoT -laitteistoa kohtaan.

3.3.1 Hyökkäysmalleja

Rodrigo ym. (2013) mainitsevat ensimmäisenä uhkana IoT:ta vastaan **palvelunesto hyökkäykset** (DoS), uhka joku löytyy myös perinteisestä Internetistä. Tosin näiden perinteisten palveluntarjoajia sekä verkkokaistaa vastaan kohdis-

tettuja palvelunesto hyökkäyksien lisäksi varsinkin IoT:ta uhkaa hyökkäys langattomien verkkojen infrastruktuuria vastaan, esimerkiksi kanavien häirintä. Myös Mohsen & Jha (2016) luokittelevat DoS -hyökkäykset vakavaksi uhaksi, ja tarkentavat Rodrigo ym. määritelmää jakamalla nämä hyökkäykset kolmeen eri tyyppiin sen mukaan miten ne vaikuttavat kohteeseen IoT:n reunalaitteistossa:

- Virtalähteen tyhjennys. IoT -laitteilla on usein rajatun kokoinen virtalähde, jos ne eivät ole suoraan yhteydessä verkkovirtaan. Tällöin DoS -hyökkäys joka kuormittaisi laitetta suuresti voisi tyhjentää sen virtalähteen, näin ollen sammuttaen sen
- Unen esto on kehittyneempi versio edellä mainitusta hyökkäys tyypistä, joka vaikeampi havaita ja torjua, sillä siinä IoT -laitteelle lähetetään suuri määrä pyyntöjä, jotka kuitenkin vaikuttavat oikeutetuilta.
- Katkos hyökkäykset voivat johtua esimerkiksi kummastakin edellisestä hyökkäysmallista, ja sen vaikutuksena laite lopettaa normaalin toimintansa. Tämä ei kuitenkaan tarkoita sitä, että laite sammuisi, vaan esimerkiksi ei kykene tunnistamaan vaaratilannetta, ja näin ollen ei sammu edes hajoamisen uhalla.

Jing ym. (2014) pitävät palvelunesto hyökkäyksiä kaikkein yleisimpänä hyökkäysmallina verkostoissa, varsinkin kun on kyse IoT:sta, johtuen verkoston heterogeenisyydestä ja monimutkaisuudesta. Heidän mukaansa tällä hetkellä ei ole hyvää ratkaisua DoS ja DDoS hyökkäyksiä vastaan.

Fyysinen vahinko on harvinaisempi uhka perinteisen Internetin näkökulmasta, mutta vakavampi IoT:lle, sillä monet laitteet voivat sijaita paikoissa joissa niihin on helppo päästä käsiksi, kuten monet sensorit (Rodrigo ym., 2013). Esimerkkinä tämän kaltaisesta sensorista voidaan käyttää aikaisemmin esimerkkinä käytettyä palohälytintä. Jos palohälyttimen sensoria vahingoitetaan, se ei kykene havaitsemaan savua, eikä laite siis toimi. Fyysiseen hyökkäykseen saattavat turvautua esimerkiksi hyökkääjät joilla ei ole teknistä taitoa toteuttaa mitään monimutkaisempaa. Mohsen & Jha (2016) mukaan fyysisten hyökkäysten vahinko riippuu laitteen tyypistä tai osasta mihin hyökkäys keskittyy. Esimerkiksi IoT:n reunalaitteiston, joka sijaitsee usein julkisissa ja helppo pääsyisissä paikoissa, tapauksessa hyökkääjällä on käytännössä mahdollista toteuttaa minkälaisia laitteen tai tiedon muokkauksia tahansa.

Salakuuntelu on passiivinen uhka, jossa hyökkääjä kerää luvattomasti tietoa verkoista aiheuttamatta niille mitään vahinkoa (Rodrigo ym., 2013). Ning ym. (2013) luokittelevat salakuuntelun keräyshyökkäykseksi. Tämän määritelmän alle kuuluvat heidän mukaansa myös tiedon käsittely tai silmäily, sekä tiedon liikenteen analysointi. Mohsen & Jha (2016) kertovat että salakuuntelu voi myös kohdistua IoT -laitteen RFID -tageihin, jolloin kaapattua tietoa käytetään esimerkiksi tagien kopioimiseen.

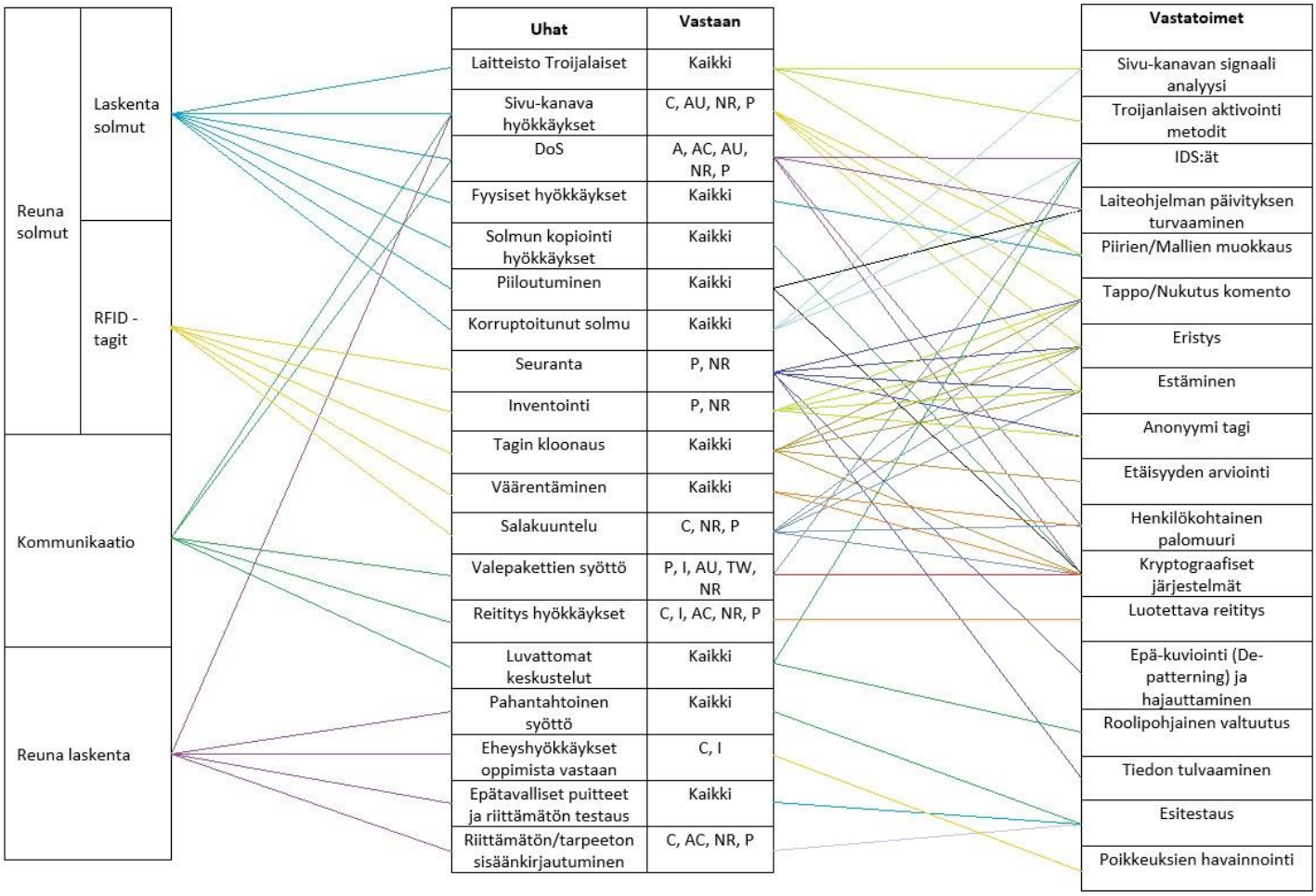
Solmukaappauksessa sen sijaan että hyökkääjä vahingoittaisi IoT -laitteita, hän tunkeutuu niiden järjestelmiin kerätäkseen tietoa, ja on aktiivinen uhka, toisin kuin salakuuntelu. Solmukaappaus voidaan myös kohdentaa fyysisten laitteiden lisäksi tiedon varastoihin tai prosessointi yksiköihin. (Rodrigo ym., 2013).

Hallinta. Pelkän vakoilun tai vahingoittamisen sijaan hyökkääjä voi myös yrittää ottaa IoT -olion hallintaansa. Tällöin vahingon määrä riippuu olion tarkoituksesta ja tärkeydestä siihen liitetyssä verkossa. Esimerkiksi kodin turvajärjestelmän hallintayksikön kaappaus saattaisi mahdollistaa koko järjestelmän sammuttamisen, muodostaen vakavan uhan. (Rodrigo ym., 2013)

Virukset, troijalaiset ja roskaposti ovat myös uhka IoT:lle samalla tavalla kuin perinteiselle Internetille (Jing ym., 2014). Nämä uhat voivat johtaa esimerkiksi tiedon vuotoon tai verkon halvaantumiseen. Ne voivat myös toimia esitoimena muun laisien hyökkäysten varalle, kuten urkinta hyökkäysten. Näiden hyökkäysten varalle tulisi verkolla olla hyvät todennus ja havainnointi mekanismit.

Hyvä tapa havainnollistaa näiden uhkien mahdollisia vaikutuksia ovat esimerkki skenaariot. Dlamini ym. (2009) esittelevät yhtenä esimerkki skenaariona uhkatilanteen terveysjärjestelmissä. Heidän esimerkissään terveyskeskuksilla ja sairaaloilla olisi järjestelmä joka muistuttaisi ihmisiä matkapuhelin kautta heitä lääkityksistä ja terveystarkastuksista. Hyökkääjä voisi kuitenkin tunkeutua tähän järjestelmään, ja muuttaa sen toimintaa siten että se lähettäisi muistutuksia väärille ihmisille, näin ollen potentiaalisesti aiheuttaen hengenvaarallisia tilanteita, kun ihmisten terveystarkastukset myöhästyisivät pahasti, tai he saisivat vääriä lääkkeitä väärien reseptien takia. Tämä esimerkki havainnollistaa hyvin miksi näiden IoT -järjestelmien suojaus on tärkeää, varsinkin niiden integroituessa nyky-yhteiskunnalle elintärkeisiin järjestelmiin, kuten terveydenhuoltoon.

Alla sijaitsevassa kaaviosta näemme miten Mohsen & Jha (2016) jakavat IoT:n uhat ja niiden vastatoimet, sekä mitä IoT:n arkkitehtuurin osaa kukin uhka vaarantaa. Kaaviosta voimme päätellä, että erilaisia uhkia on huomattava määrä.



KUVIO 2 Hyökkäysten ja vastakeinojen yhteenveto (Mohsen & Jha, 2016)

Näistä mainituista hyökkäysmalleista voidaan todeta, että monet niistä ovat paljolti samoja mitä esiintyy myös perinteisessä Internetissä, kuten palvelunesto hyökkäykset ja haittaohjelmistot. IoT:n erilaisen luonteen vuoksi kuitenkin myös muita uudenlaisia hyökkäysmalleja on olemassa, esimerkiksi fyysiset hyökkäykset eivät ole usein kovinkaan suuri uhka perinteiselle Internetille, mutta IoT -laitteistolle potentiaalisesti kyllä, koska IoT -arkkitehtuurin reunimmaiset laitteet, eli ympäristö havaitsevat ja tietoa keräävät sensorit, sijaitsevat usein paikoissa joihin niihin pääse helposti fyysisesti käsiksi.

3.3.2 Hyökkäysten motivaatiotekijöitä

Elmaghraby & Losavio (2014) esittelevät rutiini aktiviteettien teorian, jonka mukaan kolme asiaa kannustaa rikolliseen toimintaan: motivoitunut syyllinen, sopiva kohde ja toimivan suojauksen puuttuminen. Näiden kolmen elementin läsnäolo joka päiväisessä elämässä lisää rikoksen mahdollisuutta, ja puuttuminen taas vähentää sitä. Tämä määritelmä koskee rikollisuutta yleisesti, mutta on myös pätevä IoT kontekstissa.

IoT -hyökkäysten motivaatioiden voidaan sanoa paljolti olevan samoja kuin hyökkäysten perinteistä Internetiä vastaan. Mohsen & Jha (2016) kertovat että IoT on kiinnostava hyökkäysten kohde johtuen sen suuresta tiedonmäärästä ja tärkeistä järjestelmistä, joiden hallitsemiseen sen sovelluksia käytetään. Potentiaalinen hyökkääjä voi esimerkiksi olla kiinnostunut luottokortti numeroista, sijainti tiedoista, tai taloudellisten tilien salasanoista. Lisäksi hyökkääjä voi haluta hyödyntää IoT:n osioita hyökkäyksen käynnistämiseen jotain kolmatta osapuolta vastaan. Abomhara & Kien (2015) listaavat kolme asiaa jotka tekevät IoT -laitteista erittäin kiinnostavia hyökkääjien silmin.

- Suurin osa laitteistosta toimii ilman ihmisen valvontaa, joka helpottaa niiden fyysistä hyödyntämistä huomattavasti
- Komponentit usein kommunikoivat langattoman verkon kautta keskenään, joka tekee salakuuntelusta varteenotettavan uhan
- IoT -osien rajatuista resursseista johtuen niiden turvallisuus järjestelmät eivät ole kovinkaan monimutkaisia, helpottaen niihin tunkeutumista

Heidän mukaan on kuitenkin vaikea todeta yleisellä tasolla mikä motivoi hyökkäyksiä IoT:ta kohtaan tapaus kohtaisesti, sillä mahdollisia syitä on todella paljon.

4 TULEVAISUUDEN NÄKYMIÄ JA TUTKIMUKSEN AIHEITA

Yhtenä puutteena informaatioturvallisuuden tämän hetkisessä tutkimuksessa on se, että tutkijat keskittyvät paljolti kehittämään ratkaisuja nykyhetken ongelmiin ja heikkouksiin, ja näin ollen tulevaisuuden potentiaalisten ongelmien ratkaisemiseen jää vain rajoitetusti resursseja (Dlamini ym., 2009). Tämä tilanne on myös sama IoT:n turvallisuuden tutkimisessa. Myöskin Whitmore ym. (2015) ovat samaa mieltä siitä, että tämän hetken tutkimus on keskittynyt paljolti ratkaisemaan nykyisiä ongelmia, joka on tosin heidän mukaansa ymmärrettävää, sillä IoT ei ole täysin integroitunut yhteiskunnan toimintaan vielä, ja näin ollen sen tulevaisuuden turvallisuudelle ei anneta niin paljon paino arvoa kuin perinteisten verkkojen turvallisuudelle. Teknologia on jo tarpeeksi kehittynyttä, jotta IoT:n konsepti voidaan toteuttaa jossain määrin, mutta skaalautuvuus ja tehokkuus tulisivat olemaan huomattavia rajoittavia tekijöitä suuren mittakaavan toteutukselle (Atzori ym., 2010). Whitmore ym. havaintojen mukaan puutteita tutkimuksen osalta löytyy varsinkin johtamista koskevassa kirjallisuudessa, sekä lainsäädännössä ja hallinnassa. Myöskin Roman ym. (2011) mainitsevat lainsäädännön ja hallinnan olevan tärkeitä tulevaisuuden kehittämiskohteita, mutta myöskin mainitsevat niiden tasapainottamisen innovaation kanssa olevan yhtä tärkeää. Liika valvonta ja hallinta saattavat hankaloittaa innovaation syntymistä, mutta jotkin innovaatiot voivat syntyä ihmisoikeuksien hinnalla. Näin ollen rajoitukset eivät aina ole pahasta.

Whitmore ym. mukaan IoT standardien ja tutkimuksen tekemisen ja levinneisyyden osalta Eurooppa ja Aasia dominoivat muita maanosia, joka ei anna tasapainoista kuvaa tutkimuksen tekemisestä. Muita puitteita mitä he ovat havainneet IoT:n tutkimuksessa ovat IoT kirjallisuuden teknologia painotteisuus sekä IoT -pohjaisten bisnes mallien vähäisyys.

Kuten tästä tutkimuksesta on jo aikaisemmin käynyt ilmi, informaatioturvallisuus on myös yksi oleellinen tekijä, joka hidastaa IoT:n adoptointia yleiseen käyttöön (Dlamini ym., 2009). Menneisyydessä informaatioturvallisuus on myös toiminut selvänä esteenä tai hidasteena teknologian kehitykselle, mutta IoT:n kanssa on mahdollisuus ottaa se huomioon jo teknologian kehityksen alkuvaiheesta saakka, jolloin saadaan suunniteltua ja rakennettua vahva turvallisuus laitteistolle. Toisin sanoen kehityksen hidastuminen ei tässä tapauksessa ole välttämättä pahasta.

Jing ym. (2014) pitävät koko IoT -verkon turvallisuutta tärkeämpänä kuin yksittäisten laitteiden turvallisuutta, ja tämän kokonaisuuden turvallisuuden suhteen on nykyisissä tutkimuksissa puutteita. Heidän mukaansa koko verkkoa tulisi kohdella yhtenä entiteettinä turvallisuutta kehittäessä, ja ratkaisemattomia ongelmia löytyy varsinkin seuraavilta alueilta:

- Koko verkon yleinen turvallisuus. Tämä on ongelma laitteiston heterogeenisyydestä johtuen. Jokaiselle laitteelle on oma turvallisuusratkaisunsa, ja näistä erilaisista ratkaisuista voi olla hyvinkin vaikeaa rakentaa toimivaa kokonaisuutta koko verkon turvaamiseen.
- Kevyet turvallisuusratkaisut. Kuten monet muut ovat maininneet, IoT -laitteistolla ei ole käytössä paljoa resursseja raskaiden turvallisuusratkaisujen pyörittämiseen, ja tähän ei vielä ole kehitetty lopullista ratkaisua.
- Tehokkaita ratkaisuja suurille määrille heterogeenistä tietoa. IoT tuottaa valtavia määriä hyvinkin erilaista tietoa. Myöskin perinteinen Internet on menossa tähän suuntaan Big Datan tulon myötä, tosin tieto siellä on huomattavasti homogeenisempaa kuin IoT:ssa.

Abomhara & Kien (2015) huomauttavat että tulevaisuuden turvallisuuden kannalta on hyvin tärkeää ymmärtää potentiaalisten hyökkääjien motiiveja ja kykyjä, jotta pystyttäisiin vähentämään näitä uhkia ja niiden seurauksia. Tämän hetkinen tutkimus aiheesta ei heidän mukaansa ole vielä riittävää. Paljon tekemistä riittää vielä sekä käyttäjien että palveluntarjoajien puolelta. Kuten jo aikaisemmin tutkimuksessa mainittiin, hyökkääjien motivaatioiden tulkitseminen on hyvinkin vaikeaa näiden motivaatioiden monimuotoisuuden vuoksi, joka sekin on merkki lisätutkimuksen tarpeesta.

Mohsen & Jha (2014) mainitsevat vielä kaksi turvallisuus haastettua, joita ei heidän mukaansa ole aikaisemmassa kirjallisuudessa selitetty: Ensimmäisenä eksponentiaalinen kasvu heikkojen linkkien määrässä. Heidän mukaansa suurin osa IoT -pohjaisista palveluista luottavat toiminnaltaan ja varastotilaltaan rajoitettuihin patterilla toimiviin laitteisiin, ja tästä syystä markkinoilla olevista laitteista monet eivät tue erittäin turvallisia salausprotokollia. Tämä luonnollisesti johtaa siihen, että suuri osa näistä laitteista toimii heikkoina linkkeinä IoT -verkostoissa, joiden kautta potentiaalinen hyökkääjä voi päästä käsiksi turvallisempiin laitteisiin. Toinen haaste jota ei ole vielä heidän mukaansa tarpeeksi tutkittu ovat odottamattomat käyttötavat tiedolle. IoT hyödyntää suurta määrää sensoreja sen verkostojen joka päiväisessä toiminnassa, ja osaa näiden laitteiden keräämistä ja lähettämistä tiedoista voidaan käyttää eri tarkoitukseen, kun on alun perin tarkoitettu. Esimerkiksi älykodin asukkaiden tiedoista on pystytty havaitsemaan asukkaiden määrä, henkilökohtaiset elintavat ja joka päiväiset rutiinit, pelkästään lukemalla tiedot kodin sähkönkäyttöä seuraavista älymittareista.

IoT:n turvallisuus ja yksityisyys ovat myös kiinnostuksen kohdeita Euroopan Unionille, ja tästä syystä EU:lla on meneillään useita projekteja näihin aiheisiin liittyen (Sicari ym., 2014). Ensimmäisenä on Euroopan Unionin FP7 -projekti, jonka tarkoituksena on mahdollistaa älykkään ja turvallisen elämän avustus sovelluksien kehittäminen, esimerkiksi älykaupungit ja älyterveys. Toisena Sicari ym. mainitsevat Hydra -projektin, joka käsittelee muun muassa IoT:n väliohjelmiston yleisiä turvallisuus ongelmia sekä sosiaalista luotettavuutta. Kolmas projekti on uTRUSTit (Usable Trust in the Internet of Things), jonka tarkoituksena no kehittää työkaluja käyttäjille, jolla on mahdollista parantaa luotettavuuden havaitsemista IoT ympäristössä. Neljäs projekti josta Sicari ym. puhuvat on iCore,

joka tarjoaa hallinta viitekehyksen laajemmalle IoT ekosysteemille, joka on tarkoitettu kaikille IoT:n käyttäjille He myös mainitsevat muita projekteja Euroopan ulkopuolelta, kuten High Assurance Cyber Military Systems (HACMS) ohjelma USA:ssa. Kappaleen lopussa sijaitsevassa kuviossa esitellään IoT:n turvallisuuden alueita joihin edellä mainitut Eurooppalaiset projektit, sekä muutaman muu, keskittyvät.

Pahin vahinko joka on perinteisesti uhannut Internetiä, on tulonmenetys joko yrityksille tai käyttäjille (Dlamini ym., 2009). IoT -järjestelmät tulevat todennäköisesti olemaan erottamaton osa monia yhteiskunnan tärkeitä järjestelmiä, kuten terveydenhuoltoa, ja tämä mahdollistaa jopa ihmishenkien vaarantumisen, jos nämä järjestelmät pettävät huonon turvallisuuden vuoksi. Tästä syystä on tärkeää, että turvallisuus ekspertit yrittävät ennakoivasti ymmärtää ja selvittää minkälaisia uhkia IoT tulee kohtaamaan tulevaisuudessa. Nykyiset hyvin tunnetut kyberturvallisuus konseptit, kuten luottamuksellisuus, eheys ja saatavuus eivät ole nykyisellä tasolla tarpeeksi riittäviä suojaamaan IoT:ta, ja niitä tulee laajentaa esimerkiksi tiedon kulunvalvonnan osalta.

Loppujen lopuksi lähes kaikki tätä tutkimusta varten käytetty lähdemateriaali oli yhtä mieltä yhdestä asiasta: tutkittavaa ja paranneltavaa IoT:n turvallisuuden osalta löytyy kaikilta sen osa-alueilta. Kyberturvallisuus on ikuinen kilpajuoksu heikkouksien hyödyntämisen ja niiden paikkaamisen välillä, ja Esineiden Internet ei ole poikkeus tässä asiassa. Lähdemateriaalien eroavat mielipiteet tulevaisuuden kuvien suhteen löytyivät tutkimusalueiden tärkeyden painotusten osalta.

	Butler	EBBITS	Hydra	uTRUSTit	iCore	HACMS	NSF	FIRE	EUJapan
Todennus	X			X	X	X	X	X	
Luottamuksellisuus	X	X	X		X	X	X	X	X
Pääsyn hallinta	X	X		X	X	X	X	X	
Yksityisyys	X				X		X	X	X
Luottamus				X	X		X		
Toimeenpano									
Väliohjelmisto		X	X		X				
Mobiili	X						X		

KUVIO 3 Eurooppalaisten projektien kontribuutio IoT:n turvallisuuteen (Sicari ym., 2014)

5 YHTEENVETO

Tässä tutkielmassa tutkittiin Esineiden Internetin tämän hetkistä tilaa kyberturvallisuuden, ja jossain määrin fyysisen turvallisuuden, näkökulmasta. Myöskin tulevaisuuden ongelmia ja tutkimuksen aiheita käytiin läpi viimeisessä kappaleessa. Tutkimus suoritettiin kirjallisuuskatsauksena, käyttäen akateemisia lähteitä ja aiheeseen liittyviä tutkimuksia sekä kyselyitä. Tärkeimpänä tutkimustuloksena voimme huomata, että tällä hetkellä IoT tekee vielä tuloaan, ja näin ollen sen turvallisuus ei vielä ole täysin kehittynyttä, eikä siis ole verrattavissa perinteisen Internetin turvallisuuteen. Kuitenkin ympäri maailmaa on käynnissä useita projekteja ja tutkimuksia, joiden tarkoituksena on muun muassa parantaa Esineiden Internetin turvallisuutta.

Esineiden Internetin arkkitehtuuri usein jaetaan kolmeen kerrokseen niiden laitteiston ja ohjelmiston toiminnan mukaan: havainnointikerros, verkostokerros sekä käyttökerros. Jotkin tahot myös esittelevät muita kerroksia tähän jakoon, kuten väliohjelmistokerros tai liiketoimintakerros, mutta ensimmäisenä mainitut kolme ovat yleisimmässä käytössä. Kyberturvallisuuden näkökulmasta jokaisella kerroksella on omat haasteensa, joista osa vaikuttaa useampaan kerrokseen, osa ei.

IoT:lla on useita avainteknologioita, jotka ovat nykyisen tietämyksen mukaan erittäin tärkeitä sen toteutukselle. Ensimmäisinä mainitaan RFID (Radio Frequency IDentification) sekä NFC (Near Field Communication). Ne ovat kumpikin kommunikaatio teknologioita, joiden avulla IoT -laitteet voivat ottaa toisiinsa tai lähellä olevaan skanneriin yhteyden. RFID -laite on usein siru tai tagi, joka toimii IoT -laitteessa viivakoodia muistuttavalla tavalla, eli se usein sisältää laitteen tietoja, joihin päästään käsiksi skannerilla. NFC on teknologia, joka pohjautuu RFID -standardiin. NFC:n avulla laitteet voivat kommunikoida keskenään ollessaan kosketuksissa tai vähintään lyhyellä etäisyydellä toisistaan.

Sensoriverkot ovat toinen IoT:n avainteknologioista. Ne yleisesti toimivat yhteistyössä RFID -laitteiden kanssa, ja parantavat niiden kykyä havaita ympäristönsä tilaa. Sensoriverkot ovat usein langattomia, ja niiden funktiona on kerätä tietoa ympäristöstään, jota ne lähettävät eteenpäin esimerkiksi jollekin ennaltamääritellylle serverille. Sensoreille läheinen teknologia ovat aktuaattorit, jotka vaikuttavat omaan ympäristöönsä sensorien antaman tiedon perusteella. Esimerkkinä sensorien ja aktuaattorien yhteistoiminnasta löytyy palohälyttimestä, jonka aktuaattori käynnistää hälytysäänen, kun sensori havaitsee savua.

Kolmantena avainteknologiana IoT:lle toimivat pilvipalvelut. Pilvipalvelut usein jaetaan neljään eri kategoriaan: SaaS (Software as a Service), PaaS (Platform as a Service), NaaS (Networks as a Service) sekä IaaS (Infrastructure as a Service). Pilvipalvelut antavat käyttäjille mahdollisuuden hyödyntää erilaisia palveluita verkon kautta, jotka aikaisemmin olisivat sijainneet käyttäjän omissa laitteistoissa, esimerkiksi tallennustilat. IoT tulee lisäämään tiedon määrä verkostoissa huomattavasti, ja pilvipalvelut ovat tärkeä osa tämän tiedon kuljettamisen, tallentamisen ja hyödyntämisen kannalta.

Esineiden Internetille löytyy käytännön sovelluksia nykyään todella monesta eri yhteiskunnan osiosta ja palvelusta, ja tulevaisuudessa tämä sovellusten määrä tulee todennäköisesti vain kasvamaan. Esimerkkejä käytännön sovelluksista löytyy julkisesta liikenteestä, ympäristön tiedon keräämisestä ja tallentamisesta, laitteiden etähallinnasta, turvallisesta kommunikoinnista sekä lisätystä todellisuudesta. Tulevaisuudessa kokonaisia älykaupunkeja voidaan todennäköisesti rakentaa IoT:n avulla, jossa kaikki tai ainakin suurin osa palveluista ovat älykkäitä.

Esineiden Internetin kyberturvallisuutta on hyvä käsitellä kerros kerrallaan. Ensimmäisenä havainnointikerroksen turvallisuudesta. Havainnointikerroksen laitteisto sijaitsee IoT -verkon laidoilla, ja niillä on usein hyvinkin rajoitetusti käytössä laskenta-, varastointi- ja kommunikointi kapasiteettia. Tämä johtaa siihen, että näillä laitteilla on usein vain rajoitetusti vaihtoehtoja kyberturvallisuuden ratkaisujen toteuttamisessa, sillä esimerkiksi ne eivät voi käyttää kovinkaan raskaita palomuuri sovelluksia. Nämä laitteet saattavat myös sijaita ympäristössä jossa niiden valvonta on vähäistä, mahdollistaen fyysiset uhat. Mahdollisia ratkaisuja kyberturvallisuuden puolelta löytyy kevyempien turvallisuus järjestelmien kehittämisestä. Fyysistä turvallisuutta voisi auttaa esimerkiksi mikropiirien muokkaus tai itsetuho järjestelmä.

Verkostokerrokselle turvallisuus ongelmia muodostuu sen heterogeenisyydestä ja langattomasta kommunikoinnista. Heterogeeniselle laitteistolle on vaikea kehittää yhtenäistä turvallisuus ratkaisua, ja jokaiselle laitteelle oman ratkaisun kehittäminen ei ole ajallisesti ja resurssien puitteissa kovinkaan tehokasta. Langaton kommunikointi taas mahdollistaa hyökkääjien helpomman pääsyn käsiksi siinä kulkevaan tietoon, kuin perinteisessä langallisessa verkossa. Ratkaisuja verkostokerroksen turvallisuudelle löytyisi esimerkiksi luotettavan reitityksen rakentamisesta, IDS:n (Intrusion Detection System) käyttämisestä, sekä tulvinta perusteisesta liikenteenvastaisesta analyysi mekanismista.

Käyttökerroksen ongelmat muodostuvat myöskin laitteiston heterogeenisyydestä, sekä myös käyttäjien yksityisyyden turvaamisesta. Käyttökerroksessa sijaitsevat käyttäjien päätelaitteet, joille aiheutuu turvallisuusongelmia niiden suuresta vaihtelevuudesta. Koska käyttäjät joko käyttävät laitteitaan tietojen varastoitiin tai siirtämiseen toiseen laitteeseen, yksityisyys on vakava ongelmatekijä. Myöskin vaaditun tiedon tarkkuus ja rajatut resurssit aiheuttavat ongelmia, sekä pilvipalvelut, sillä useat käyttökerroksen laitteet hyödyntävät pilvipalveluita toiminnassaan, ja näin ollen joutuvat luottamaan näiden palveluiden turvallisuusratkaisuihin omiensa sijaan.

Turvallisuus Esineiden Internetissä sisältää useita osa-alueita ja konsepteja. Ensimmäisinä näistä tutkielmassa esitellään yksityisyys, tiedon keräys ja säilytys. IoT:n takia tiedon ja käyttäjien määrä verkostoissa kasvaa räjähdysmäisesti, ja tämä tietysti vaikeuttaa kaikkien käyttäjien tietojen yksityisyyden ylläpitämistä ja säilyttämistä. Yksi mahdollinen ratkaisu tähän on asettaa lainsäädännöllisiä rajoituksia tiedon keruuseen ja säilytykseen, sekä tarjota käyttäjille työkaluja joiden avulla he voivat itse määrittää näitä rajoituksia. Mitkään lait eivät kuiten-

kaan auta laittomaan tiedon keräykseen, ja tästä syystä laitteille pitää myös kehittää toimivia turvallisuus- ja salausjärjestelmiä. Ongelmia tässä taas kerran aiheuttaa laitteiston heterogeenisyys ja suuri määrä.

Seuraavina konsepteina mainitaan identiteettien hallinta ja luottamus. IoT:n laitteiden suuri määrä vaatii suuren määrän identiteettejä, sillä kaikki laitteet vaativat vähintään yhden identiteetin, toiset enemmänkin. Tässäkin ongelmaksi muodostuu laitteiston heterogeenisyys, koska laitteiden erilaisuus tarkoittaa, että identiteettienkin pitää olla uniikkeja. Perinteiset Internetin nimeämiskeinot eivät siis riitä IoT:lle. Yksi ratkaisu tähän on ihmisten ja laitteiden todennusjärjestelmien yhdistäminen, eli laite olisi sidottu johonkin käyttäjän identiteettiin. IoT:n kontekstissa luottamus tarkoittaa laitteiden välisen tai käyttäjän ja laitteen kanssakäymisen epävarmuutta. Mitä suurempi luottamus, sitä paremmalta käyttäjältä tuntuu toimia IoT -ympäristössä. Tästä syystä käyttäjille olisi hyvä tarjota jonkinlaisia työkaluja ympäristönsä hallitsemiseen rajoitetussa määrin. Myöskin jonkinlainen hallinta palveluntarjoajan puolelta olisi hyvä ratkaisu, tosin sillekin täytyisi asettaa rajoituksia, jottei väärinkäytöksiä syntyisi. Yksi ratkaisu käyttäjien luottamuksen parantamiseksi olisi luottamuspiiri, jossa käyttäjät voisivat arvioida toistensa luotettavuutta, ja näin antaa heille oikeuksia toimia.

Viimeisenä käsiteltynä konseptina on vikasieto, joka tarkoittaa laitteiden kykyä toimia virheistä huolimatta. IoT -laitteiston suuresta määrästä johtuen, vikojen ilmentyminen joihinkin niistä elinkaaren aikana on suorastaan välttämätöntä. Myöskin laitteiston rajoitetut resurssit parantavat vikojen ilmestymismahdollisuuksia. Vikasiedon saavuttamiseksi on ehdotettu kolmea yhteistoiminnallista asia: laitteiden tulee olla oletuksena turvallisia, laitteiden tulee nähdä kytketyn verkon ja sen palveluiden tila, sekä laitteiden tulee kyetä puolustautua verkon kaatumista tai hyökkäyksiä vastaan.

Hyökkäysmalleja IoT -kokonaisuutta vastaan on useita, joista osa on uhkia kaikille arkkitehtuurin kerroksille, toiset vain osalle laitteistosta. Yksi yleisimpiä uhkia ovat palvelunesto hyökkäykset. Muita uhkia esimerkiksi ovat fyysinen vahinko, salakuuntelu, solmukaappaus, hallinta, virukset, troijalaiset sekä roskaposti. Hyökkäysmallien uhkaa on hyvä havainnollistaa esimerkki skenaarioilla, kuten sairaalan toiminnan häiritseminen ja potilastietojen muokkaaminen

Hyökkääjien motivaatiot hyökkäysten toteuttamiseen ovat monimuotoisia. Periaatteessa samat tekijät pätevät kuin muussakin kyberrikollisuudessa, painotuksena tietojen urkkiminen tai väärentäminen IoT:n sisältämän suuren tietomäärän vuoksi. Myöskin laitteiden vähäinen valvonta, langaton kommunikointi sekä rajatut resurssit kannustavat hyökkäyksiä niitä vastaan.

Esineiden Internetin tulevaisuuden näkymiä hallitsee lisätutkimuksen tuottamisen tarve. Kaikilla turvallisuuteen liittyvillä aihealueilla on vielä paljon tutkittavaa jäljellä ennen kuin voidaan puhua hyvästä turvallisuudesta, esimerkkinä vaikka teknologia jo riittää IoT -konseptin toteuttamiseen suurissa määrin, skaalautuvuus ja tehokkuus tulisivat aiheuttamaan ongelmia. Myöskin potentiaalisia hyökkääjiä, heidän metodejaan ja motiiveja tulisi tutkia lisää, jotta oikean-

laisia vastakeinoja osattaisiin kehittää. Tällä hetkellä käynnissä on useita projekteja ympäri maailmaa, joilla ainakin yhtenä tavoitteena on kehittää Esineiden Internetin turvallisuutta.

Tämän tutkielman suurin heikkous tulee sen yleisluontoisuudesta. Tutkielmassa käytiin läpi Esineiden Internetin yleisin arkkitehtuuri jako ja sen turvallisuus, mutta muitakin mahdollisia jakoja on esitetty, niin kuin lyhyesti tutkielmassa mainittiin. Sama pätee myös hyökkäysmallien ja motiivien kanssa, sillä on olemassa muitakin vaihtoehtoja kuin esitellyt. Tähän tutkielmaan kasattiin näistä vain yleisimmät, ja annettiin niistä lyhyt esittely esimerkkien kanssa. Esineiden Internet on jo nyt, ja tulee olemaan, valtavan suuri verkosto hyvinkin erilaisia laitteita, joilla monilla tulee olemaan hyvinkin erilaiset vaatimukset turvallisuuden suhteen. Yhdistävinä tekijöinä voidaan yleisesti puhua laitteiston rajatuista resursseista ja niiden verkkoriippuvuudesta, jotka ovat myös erittäin rajoittavia tekijöitä turvallisuuden kannalta. Kaikkien mahdollisten ongelmien ja ratkaisujen läpikäyminen vaatisi huomattavasti kattavamman tutkielman, joka ylittäisi kandidaatintutkielman vaatimukset selvästi.

Tätä tutkielmaa voitaisiin kuitenkin käyttää tutustuttamaan lukija Esineiden Internettiin ja sen turvallisuuden peruskäsitteisiin. Tutkielmaa voitaisiin myöskin hyödyntää lisätutkimusta kaipaavien aihealueiden paikallistamiseen IoT:n turvallisuuden suhteen.

LÄHTEET

Aazam, M., Khan, I., Alsaffar, A. A., & Huh, E. N. (2014, January). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014* (pp. 414-419). IEEE.

Abomhara, M., & Kien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security*, *4*, 65-88.

Alcaide, A., Palomar, E., Montero-Castillo, J., Ribagorda, A. (May 2013). Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security (2012) 37, 111-123

Atrozi, L., Iera, A., Morabito, G. (June 2010). The Internet of Things: A survey. Computer Networks (2010) 54, 2787-2805

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. *Journal of urban technology*, *18*(2), 65-82.

Chen, D., Chang, G., Jin, L., Ren, X., Li, J., & Li, F. (2011, August). A novel secure architecture for the Internet of things. In *Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on* (pp. 311-314). IEEE.

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), 349-359.

Dlamini, M. T., Eloff, M. M., & Eloff, J. H. P. (2009, August). Internet of things: emerging and future scenarios from an information security perspective. In *Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2009)* (p. 6).

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, *24*(2), 381–394. doi:10.1109/jsac.2005.861395

Khoo, B. (October 2011). RFID as an enabler of the internet of things: issues of security and privacy. In Internet of Things (iThings/CPSCom), 2011 Interna-tional Conference on and 4th International Conference on Cyber, Physical and Social Computing (pp. 709-712). IEEE.

Mohsen Nia, A., & Jha, N. K. (2016). A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*. doi:10.1109/tetc.2016.2606384

Nam, T., & Pardo, T. A. (2011, June). Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times* (pp. 282-291). ACM.

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. *Computer*, 4, 46-53.

Ozturk, C., Zhang, Y., & Trappe, W. (2004, October). Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 88-93). ACM.

Rodrigo, R., Jianying, Z., Lopez, J. (March 2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks (2013) 57, 2266-2279

Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer*, *44*(9), 51-58.

Rui, W., Jinguo, W., & Na, W. (2015). Analysis of key technologies in the Internet of things.

Sarma, A. C., Girão, J. (March 2009). Identities in the Future Internet of Things. Wireless Pers Commun (2009) 49, 353–363

Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. (November 2014). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks (2015) 76, 146-164

Suo, H., Wan, J., Zou, C., & Liu, J. (March 2012). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 3, pp. 648-651). IEEE.

Takaragi, K., Usami, M., Imura, R., Itsuki, R., & Satoh, T. (2001). An ultra small individual recognition security chip. *IEEE micro*, *21*(6), 43-49.

Want, R. (2011). Near field communication. *IEEE Pervasive Computing*, *3*(10), 4-7.

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

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 Communication Systems*, *25*(9), 1101.

Zhang, B., Ma, X. X., & Qin, Z. G. (2011). Security architecture on the trusting internet of things. *Journal of Electronic Science and Technology*, *9*(4), 364-367.

Zhang, Z. K., Cho, M. C. Y., & Shieh, S. (2015, April). Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (pp. 1-6). ACM.