Tampereen yliopisto

Aleksi Lahtinen

IOT-LAITTEIDEN TIETOTURVA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Maaliskuu 2020

TIIVISTELMÄ

Aleksi Lahtinen: IoT-laitteiden tietoturva
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Maaliskuu 2020

Tässä tutkielmassa tarkastellaan IoT-laitteiden, eli esineiden internet -laitteiden tietoturvaa ja niihin liittyviä tietoturvaongelmia. Tarkoituksena on löytää syitä IoT-laitteiden tietoturvaongelmiin sekä esitellä näitä ongelmia. Tutkielmassa selviää, että IoT on kasvattanut suosiotaan nopeasti, jonka takia myös IoT-laitteiden määrä on kasvanut todella suureksi. Nopea kasvu ja laitteiden suuri määrä myös johtuvat suurelta osin siitä, että käytännössä mikä tahansa verkkoon liittyvä laite voidaan luokitella IoT-laitteeksi. Tutkielman yhtenä löydöksenä voidaan kuitenkin havaita, että IoT:n nopeasta kasvusta huolimatta IoT:n kasvu olisi voinut olla entistäkin nopeampaa. Suurena syynä tälle on esitetty IoT-laitteita vaivaavat tietoturvaongelmat. Tämä on näkynyt esimerkiksi siten, että kuluttajamarkkinoille on julkaistu paljon IoT-laitteita, joita vaivaavat erinäiset tietoturvaongelmat. Yksi perimmäisistä syistä tähän on ollut yritysten taloudellisten voittojen tavoittelu tietoturvan ja sen testauksen kustannuksella.

Käytännössä IoT-laitteiden tietoturvaongelmat liittyvät usein käyttäjän henkilökohtaisen datan vaarantumiseen tai pääsemiseen vääriin käsiin. Tietoturvaongelmia havainnollistetaan esimerkkien avulla käyttäen muun muassa puhelinta ja Web-kameraa. Tämän tutkielman lopputuloksena löydetään useita eri tietoturvaongelmia, jotka liittyvät IoT:n eri osa-alueisiin ja vaikuttavat IoT-laitteiden toimintaan eri tavoilla.

Aihe on ajankohtainen ja mielenkiintoinen, koska IoT on tällä hetkellä suuressa suosiossa ja sillä on paljon potentiaalia. IoT-laitteet tulevat jatkuvasti myös yhä näkyvämmäksi osaksi tavallisen käyttäjän arkea, koska käytännössä mikä tahansa elektroninen laite voi olla IoT-laite. Tämän lisäksi tietoturva on sellainen asia, johon on alettu kiinnittämään huomiota entistä enemmän ja se puhuttaa tavallistenkin ihmisten keskuudessa.

Avainsanat: IoT, IoT-laite, Tietoturva, Tietoturvaongelma, Tietoturvavaatimus, Yksityisyys, Verkko

1 Johdanto

IoT (Internet of Things), eli esineiden internet on kasvattanut suosiotaan nopeasti viime vuosien aikana ja uusia IoT-laitteita tulee jatkuvasti markkinoille. Tämä näkyy esimerkiksi siten, että nykyisin käytännössä mikä tahansa sähköinen tai akkukäyttöinen laite voi olla IoT-laite. Tämän kandidaatintyön tarkoituksena on tutkia IoT-laitteiden tietoturvaa ja etenkin sitä, minkälaisia tietoturvariskejä IoT-laitteisiin kohdistuu. Tämä työ on kirjallisuuskatsaus IoT-laitteiden tietoturvaan ja niihin kohdistuviin tietoturvariskeihin.

Käytettyjä lähteitä on pääasiallisesti haettu Tampereen yliopiston kirjaston Andor-tiedonhakupalvelusta, mutta myös Google Scholarin kautta. Mikäli Google Scholarista löytyi potentiaalinen lähde, on sen saatavuus tarkastettu aina Andor-tietokannasta. Hakuja on muun muassa tehty käyttäen hakusanoja ”IoT Security”, ”IoT Challenges”, ”IoT Security Issues”, ”IoT Privacy” ja ”IoT”. Parhaimmat tulokset löytyivät hakusanoilla ”IoT Security” ja ”IoT Security Issues”. Löydöksiä on pyritty karsimaan sen mukaan, jos esimerkiksi sanat ”Security” tai ”Privacy” puuttuivat kokonaan hakutuloksesta. Samoin, jos hakutuloksessa käsiteltiin yksinomaan esimerkiksi kodin elektroniikkaa, on tämän tyyppisiä tuloksia pyritty karsimaan. Käytettyjen lähteiden ensisijaisena tarkoituksena on ollut se, että ne eivät sitoutuisi mihinkään yhteen laitteistoryhmään, vaan käsittelevät IoT:ta ja IoT-laitteita yleisellä tasolla. Koska tässä työssä on myös aiheen takia melko paljon teknistä sanastoa, on näitä termejä pyritty määrittelemään Googlen kautta etsityillä hakutuloksilla.

Luvussa 2 määritellään se, mitä IoT tarkoittaa ja minkälaisia IoT-laitteita voi olla olemassa. Tämän lisäksi tässä luvussa täsmennetään se, mitä tietoturva, tietosuoja ja kyberturvallisuus ovat. Luvussa 3 tarkastellaan IoT-laitteiden tietoturvaa yleisellä tasolla ja perehdytään muun muassa siihen, miksi kuluttajamarkkinoilla on paljon IoT-laitteita, joissa on tietoturvaongelmia. Tämän lisäksi tässä luvussa käsitellään esimerkkien avulla sitä, miten IoT-tietoturvaongelmat voivat käytännössä näkyä. Luvut 4 ja 5 ovat tämän työn teknisimmät luvut ja niissä paneudutaan tarkemmin erilaisiin protokolliin, standardeihin, tietoturvavaatimuksiin ja arkkitehtuurillisiin asioihin, jotka liittyvät IoT-laitteisiin. Luvussa 6 esitellään konkreettisia tietoturvaongelmia, joita IoT-laitteissa esiintyy. Luvussa 7 ovat tämän työn yhteenveto ja pohdinnat.

2 IoT ja tietoturva

Tässä luvussa määritellään, mitä IoT ja tietoturva tarkoittavat. Tietoturvaan myös liittyvät osittain termit kyberturvallisuus ja tietosuoja, jotka myös käsitellään tässä luvussa. Tietoturva ja IoT ovat käytännössä tämän tutkielman tärkeimpiä termejä, joita käytetään jatkuvasti myöhemmissä luvuissa.

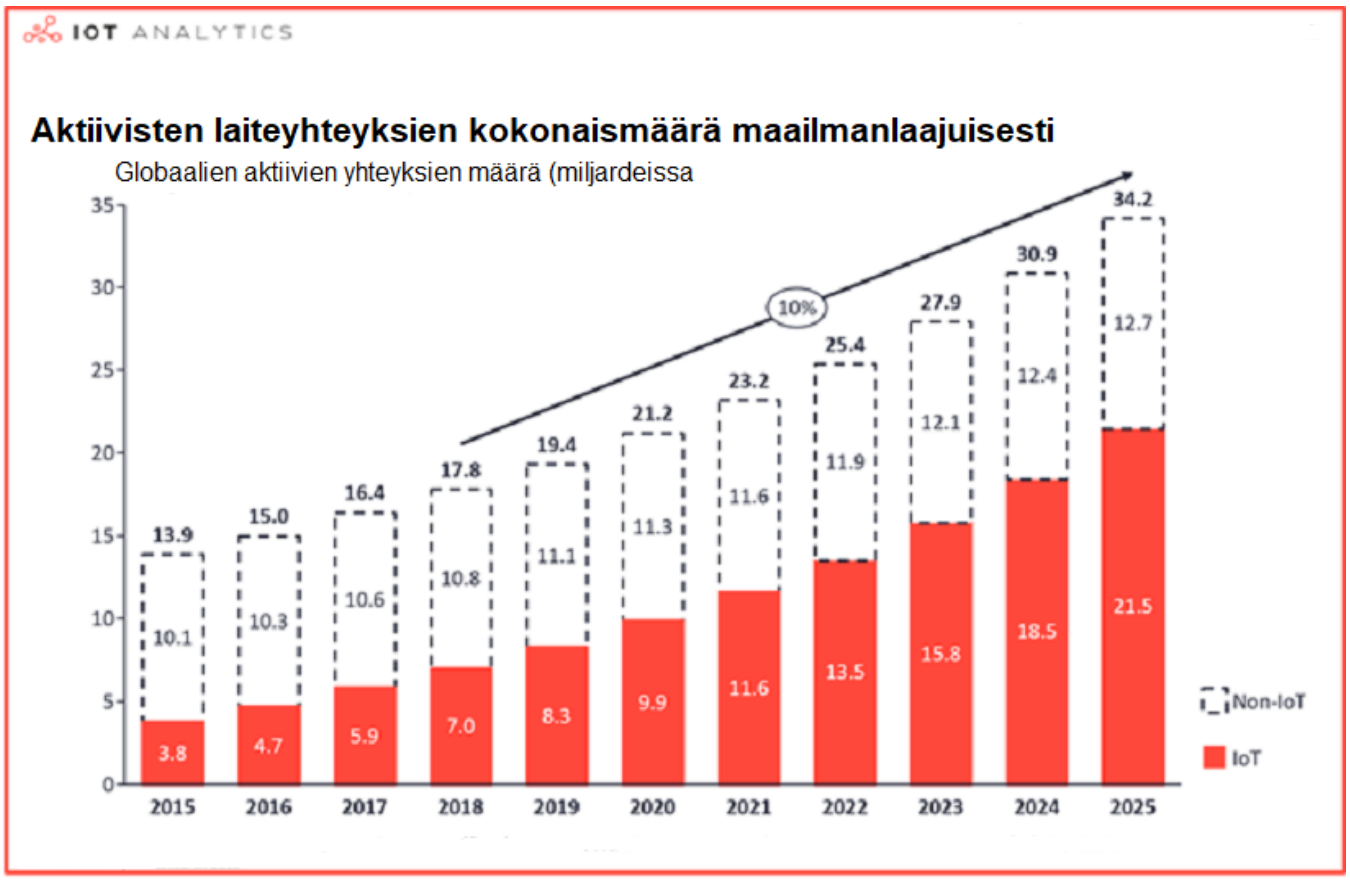
2.1 IoT:n määritelmä

Kuvittele maailma, jossa käytännössä mikä tahansa asia voi olla kytkettynä verkkoon kommunikoiden keskenään ja ihmisten kanssa tuoden mukanaan uusia palveluita, jotka parantavat jokapäiväistä elämäämme. Itsestään ajavat dronet, jotka tuovat ostoksesi kotiovellesi ja vaatteet, jotka pystyvät mittamaan terveyttäsi ovat kaikki osa suurta teknologista muutosta, jota kutsutaan nimellä Internet of Things (Esineiden internet). [Hanes et al., 2017.]

IoT on konsepti, jossa mikä tahansa laite yhdistyy verkkoihin ja niiden kautta toisiin laitteisiin. IoT on jättimäinen verkosto laitteita ja ihmisiä, jotka kaikki keräävät ja jakavat dataa toiminnastaan sekä ympäröivästä ympäristöstä. [Clark, 2016.]

IoT:n tavoitteena on yhdistää kaikki laitteet Internettiin, jotta ne voivat kommunikoida ja olla vuorovaikutuksessa keskenään sekä ihmisten kanssa. IoT on teknologiasiirtymä, jossa laitteiden avulla voimme aistia ja hallita fyysistä maailmaa tekemällä esineitä älykkäämmiksi ja yhdistämällä niitä älykkäisiin verkkoihin. [Hiebert, 2013.]

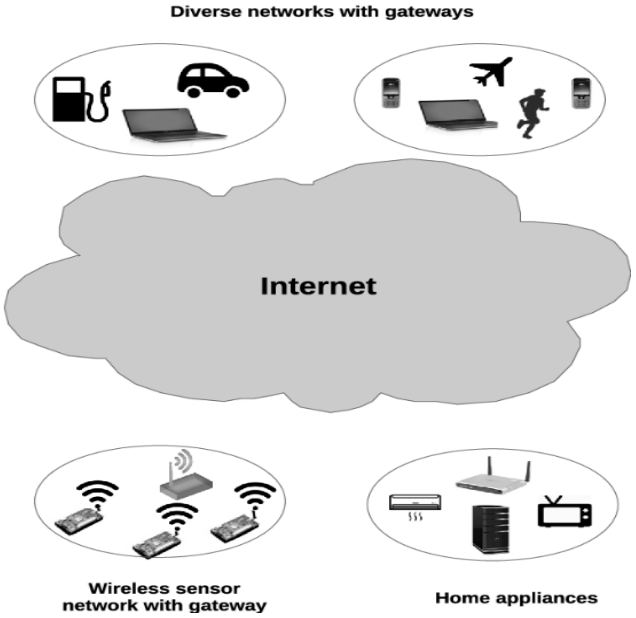
IoT on kasvattanut suosiotaan nopeasti viime vuosien aikana, ja se myös on kerännyt ympärilleen paljon keskustelua. Lueth [2018] ilmoitti jo vuonna 2018 verkkoon yhdistyneitä laitteita olevan 17 miljardia kappaletta, joista IoT-laitteiden osuus oli 7 miljardia. Tämän määrän oletetaan kasvavan 22 miljardiin kappaleeseen vuoteen 2025 mennessä, kuten kuvassa 1 on osoitettu. Raju kasvu ja suuri määrä johtuvat siitä, että käytännössä mikä tahansa laite voidaan luokitella IoT-laitteeksi, kuten puhelimet, tabletit, televisiot, kodin elektroniikka ja moni muu.



Kuva 1. IoT-laitteiden määrä (Valkoisella merkityt ovat verkkoihin yhdistyneet laitteet, jotka eivät ole IoT-laitteita. Punaiset ovat IoT-laitteita). [Lueth, 2018].

Gilcrhrist [2017] toteaa IoT:n olevan käsitteenä todella laaja-alainen, sillä se pitää sisällään suuren määrän monenlaisia Internet-yhteyteen kykeneviä asioita, kuten lamppuja, autoja ja kodinturvalaitteita. Hän [Gilcrhrist, 2017] myös linjaa, IoT:n olevan laaja käsite, koska sen alaisuuteen voidaan luokitella nykyisin käytännössä mikä tahansa tekninen laite löyhin perustein. Clarkin [2016] ja Hiebertin [2013] määritelmistä on myös havaittavissa, että IoT on käsitteenä hyvin laaja, eikä sille löydy täysin selkeää ja yksiselitteistä määritelmää, joka tukee Gilchristin [2017] näkemystä IoT:sta.

Tyypillinen IoT-laitteiden toimintaympäristö pitää sisällään heterogeenisiä laitteita sisäänrakennetuilla sensoreilla, jotka ovat kytkeytyneet toisiinsa verkon kautta, kuten kuvassa 2 on esitetty. IoT-laitteet ovat yksilöitävissä ja niille tyypillisesti ominaista on pieni virrankulutus, pieni muistin määrä ja rajoitettu prosessointiteho. Portteja tai yhdyskäytäviä käytetään yhdistämään IoT-laitteita ulkomaailmaan tietojen ja palvelujen etätoimittamiseksi IoT-käyttäjille. [Khan ja Khaled 2017.]



Kuva 2. IoT-laitteiden toimintaympäristö. [Khan ja Khaled 2017: 396].

Kuten millä tahansa nopeasti kasvavalla innovaatiolla, ilmiöllä tai tuotteella, on IoT:lla myös omat ongelmakohtansa. IoT:n tietoturva ja sen heikohko taso on herättänyt paljon keskustelua ympärilleen. Hanes ja muut [2017] kertovat tutkijoiden löytävän jatkuvasti uusia tietoturvariskejä kuluttajalaitteista ja nopeana ratkaisuna laite usein eristetään verkosta ja muista laitteista, joka on kuitenkin vastoin kaikkia IoT:n perusperiaatteita. Hanes ja muut [2017] myös linjaavat, että IoT:n tarkoituksena on luoda luotettava verkosto, jossa itsenäiset ja heterogeeniset laitteet kommunikoivat ja tekevät yhteistyötä keskenään.

2.2 Kyberturvallisuus ja tietoturva

Tietoturva on ollut terminä tunnettu jo vuosikymmeniä, ja tämän lisäksi uudempana terminä myös tunnetuksi on tullut kyberturvallisuus. Ne liittyvät käytännössä kahteen eri asiaan, mutta menevät helposti sekaisin keskenään. Tähän liittyen Puro [2017] linjaa, että helpointa hahmottaa näiden kahden termin eroa on ajatella, että tietoturva liittyy ja

käsittelee tiedon, eli datan turvaamista. Tiedoksi luokitellaan esimerkiksi sähköpostit, tiedostot ja tunnukset eri palveluihin. Puro [2017] antaa esimerkkeinä tieto-ominaisuuteen kohdistuvista uhkista ympäröivän tilan heikon fyysisen turvallisuuden tai heikon verkkoturvallisuuden, joka voi altistaa siinä olevat laitteet tietomurroille. Tietoturvaa ja sitä, miten se liittyy IoT-laitteiseen, käsitellään tarkemmin seuraavissa luvuissa. Esimerkiksi kodassa 3.2 annetaan konkreettisia esimerkkejä siitä, miten tietoturvaan liittyvät ongelmat voivat käytännössä näkyä IoT-laitteissa.

Puro [2017] täsmentää kyberturvallisuuden eron tulevan siinä, että se kattaa tietoturvallisuuden alueista verkkojen kautta tehtävät tietomurrot ja tietojärjestelmien varassa toimivan infrastruktuurin turvallisuuden. Hän antaa esimerkkinä tästä sähköautojen ohjausjärjestelmät, teollisuuslaitosten prosessiautomaatiojärjestelmät ja autonomiset ajoneuvot.

Tietosuoja (Data privacy) tarkoittaa yksityisyyden suojaan, joka liittyy datan asianmukaiseen käsittelyyn ja siihen liittyviin suostumuksiin, ilmoituksiin ja sääntelyvelvoitteisiin. Käytännön tietosuojaongelmat liittyvät usein seuraaviin: Jaetaanko tietoja kolmansien osapuolten kanssa, kuinka tietoja laillisesti kerätään tai säilytetään ja sääntelyrajoitukset, kuten GDPR (General Data Protection Regulation). [Petters, 2020.]

Alsted ja Flinck [2018] täsmentävät, että GDPR on EU:n yleinen tietosuoja-asetus, joka muun muassa asettaa yrityksille ja organisaatioille velvollisuuksia siihen, miten henkilötietoja käsitellään. Alsted ja Flinck [2018] lisäävät tähän, että GDPR helpottaa ihmisten mahdollisuuksia kontrolloida omia henkilötietojaan, kuten oikeus siirtää omat tiedot tietojärjestelmästä toiseen. Tietosuojaa sekä tietoturvaa ja niiden yhteyttä IoT-laitteisiin käsitellään tarkemmin luvussa 5, jossa esitellään erilaisia IoT:n tietoturvavaatimuksia, joihin myös tietosuoja liittyy. Tietosuoja on oleellinen osa näitä vaatimuksia.

3 Yleistä IoT-laitteista ja niiden tietoturvasta

Tässä luvussa käsitellään tarkemmin IoT-laitteiden tietoturvaa ja sitä, että miksi kuluttajamarkkinoille on päässyt paljon sellaisia IoT-laitteita, joiden tietoturva on heikolla tasolla. Tämän lisäksi tässä luvussa käytetään esimerkkejä kuvastamaan, miten tietoturvaongelmat voivat käytännössä näkyä IoT-laitteita käytettäessä.

3.1 Miksi markkinoilla on paljon heikon tietoturvan omaavia IoT-laitteita?

Vaikka IoT on kasvanut nopeasti nopeasti, olisi sen kasvu voinut olla entistäkin nopeampaa. Yhtenä suurimpana syynä tähän on pidetty IoT-laitteita vaivaavia tietoturvaongelmia. IoT:n odotuksia hitaampi kasvu on myös johtunut osittain siitä, että monet yritykset halusivat nopeasti mukaan IoT:n buumiin taloudellisten voittojen toivossa. Tämä puolestaan johti tilanteeseen, jossa kuluttajamarkkinoille pääsi paljon tuotteita joiden tietoturva oli heikolla tasolla. Heikko tietoturva vaikutti negatiivisella tavalla kuluttajien luottamukseen IoT-laitteita kohtaan. [Gilchrist, 2017.]

Ymmärtääksemme enemmän siitä, miksi markkinoille on päässyt paljon IoT-laitteita, joissa on tietoturvaongelmia, on tätä asiaa myös tarkasteltava tuottajan näkökulmasta. Gilchrist [2017] selvittää kehittäjien suunnittelevan monia IoT-laitteita lyhyellä kehitysajalla ja näiden laitteiden tarkoituksena on vain selvittää jonkin idean toteuttamiskelpoisuutta, eikä julkaista valmista tuotetta markkinoille. Gilchrist [2017] linjaa, että valitettavasti tästä huolimatta liiketoiminnan tarpeet ja taloudelliset rajoitukset ajavat monet tuotteen markkinoille julkaistavaksi ennen aikojaan, jotta yritys voisi saada julkista kiinnostusta tai ollakseen ensimmäinen vastaavan tuotteen kanssa markkinoilla. Tämä puolestaan johti Gilchristin [2017] mukaan siihen, ettei laitteen kehittäjillä ollut riittävästi aikaa testata, toteuttaa ja validoida tuotteen ohjelmistoja, laitteistoja ja firmwarea (laiteohjelmisto). Fisher [2019] täsmentää firmwaren tarkoittavan ohjelmistoa, joka on rakennettu laitekohtaisesti jollekin yksittäiselle laitteelle. Se sisältää joukon ohjeita siitä, miten laitteen tulisi toimia ja kommunikoida toisten laitteiden kanssa.

Nykyisin ohjelmistoja ja tuotteita kehitetään IT-alalla yleisesti niin kutsutuilla ketterillä menetelmillä. Tämä tarkoittaa käytännössä sitä, että tuotetta kehitetään iteratiivisesti osissa ja kunkin iteraation päätteeksi tuotteeseen lisätään jotakin uutta, kuten päivitetty toiminnallisuus sen ohjelmistoon. Tässä voi syntyä kulttuurien yhteenotto, jossa laitteen tai ohjelmiston kehittäjät haluavat testata laitetta mahdollisimman paljon löytääkseen mahdollisia tietoturvaongelmia ja ohjelmistovirheitä, kun taas myyjät ja markkinointi haluavat saada laitteen tai ohjelmiston mahdollisimman nopeasti markkinoille tuottamaan rahaa. Tämän tyyppisessä tilanteessa ylin johto on valinnan edessä, jossa joko tuote julkaistaan mahdollisten puutteiden kanssa tai sitten se jätetään vielä kehitykseen, joka puolestaan voisi kestää vielä useampia iteraatioita. Useampienkin iteraatioiden jälkeen tuotetta ei silti välttämättä pidettäisi valmiina julkaistavaksi. [Gilchrist, 2017.]

3.2 Miten tietoturvaongelmat voivat näkyä käytännössä?

Nykyisin laitteet kuten tulostimet, reitittimet, puhelimet ja monet muut sähköiset laitteet ovat kaikki yhteydessä toisiinsa käytön ja ylläpidon helpottamiseksi, mutta samalla kasvavat tietoturvariskit. Pääsy näiden laitteiden kautta kerättyyn dataan voi auttaa rikollisia tai muita ei haluttuja osapuolia pääsemään käsiksi arkaluontoisiin asioihin, kuten potilastietoihin tai kameroiden keräämään videomateriaaliin. [Agarwal et al., 2019.]

Näkyväksi ongelmaksi voidaan nostaa erityisesti puhelimet ja niiden kautta ladattavat sovellukset esimerkiksi Applen tai Googlen sovelluskaupoista. Puhelimeen ladattavilla sovelluksille on tyypillistä, että ne vaativat toimiakseen käyttöoikeuksia, jotka voivat vaatia pääsyä puhelimen dataan, kameraan, mikrofoniin, GPS-tietoihin, sähköpostiin tai jopa viesteihin. Nämä käyttövaatimukset näytetään usein listana käyttäjälle, kun hän ensimmäistä kertaa käynnistää sovelluksen. Tässä muodostuu olennaiseksi ongelmaksi se, kun käyttäjillä on usein kiire päästä käyttämään uutta sovellusta ja he hyväksyvät nämä ehdot lukematta niitä. Tällä toiminnalla käyttäjä voi tiedostamattaan altistaa jopa arkaluontoista dataa sellaisille tahoille, joiden ei olisi muuten tarkoitus päästä niihin käsiksi. [Gilchrist, 2017.]

Koska IoT-laitteilla, kuten puhelimilla on usein pääsy käyttäjän henkilökohtaiseen dataan, muodostuu siinä Adascalitein [2019] mukaan niiden suurin ongelma, koska ne eivät ole lähtökohtaisesti kovin turvallisia ja niitä vastaan voidaan tehdä monenlaisia tietoturvahyökkäyksiä. Tämä muodostaa laitteen käyttäjälle suuria riskejä, joka voi johtaa henkilökohtaisten tietojen vuotamiseen tai jopa taloudellisiin menetyksiin. Tähän liittyen Agarwal ja muut [2019] lisäävät, että oleellisimmat syyt tietoturvaongelmiin löytyvä IoT:n suunnitteluperiaatteista. Agarwal ja muut [2019] täsmentävät, ettei IoT-laitteissa ole keskeisiä tietoturvaratkaisuja, kuten palomuureja, virustorjuntaohjelmia tai mitään muita tyypillisiä keinoja tietoturvariskien havaitsemiseen. Tähän Agarwal ja muut [2019] lisäävät, että IoT-laitteissa on laitteistokohtainen firmware ja jokainen laite käyttää usein omia protokollia, jotka ohjaavat laitteen toimintaa. Koska IoT-laitteet keräävät paljon dataa, tähän liittyen Agarwal ja muut [2019] täsmentävät, että laitteiden firmwarejen tulisi olla kehitetty siten, että ne ovat turvallisia, mutta tämä toteutuu vain harvoin. Puhelimissa ja tableteissa on saatavilla erilaisia virustorjuntaohjelmistoja, joten tässä yhteydessä olettaisin, että Agarwal ja muut [2019] puhuvat muista IoT-laitteista, kuten kodin elektroniikasta.

IoT-laitteiden nopeasti kasvava lukumäärä mahdollistaa uusia hyökkäysmenetelmiä ja rajapintoja rikollisten sekä hakkereiden käyttöön, joka aiheuttaa vakavia riskejä liittyen tietoturvaan ja käyttäjän yksityisyyteen. IoT-laitteisiin kohdistuvat käytännön hyökkäykset ovat myös jo osoitettu todellisiksi uhkiksi. Jo vuonna 2014 asiantuntijat demonstroivat, miten verkkoon liitetyn hehkulampun kautta oli mahdollista saada Wi-Fi tunnukset ja salasanat taloudesta, jossa valaisin oli käytössä. Hyökkäyksiä on myös kohdistunut etäluettaviin sähkömittareihin, kodin automaatiolatteisiin, ja vuonna 2015 autovalmistaja Chrysler joutui lähettämään tietoturvapäivityksen kaikille asiakkailleen. Chryslerin autoista paljastui vakava haavoittuvuus, jossa auton moottoria, jarruja ja rattia voitiin kauko-ohjata autosta löytyvän viihdejärjestelmän kautta. [O'Neill, 2016.]

3.3 IP-kameran tapaus

Seralathan ja muut [2018] suorittivat tutkimuksen, jossa käytettiin tavallista IP-kameraa (Internet Protocol Camera), eli toisin sanoen Web-kameraa havainnollistamaan sitä, minkälaisia tietoturvariskejä vastaava laite voisi käytössä aiheuttaa. Lisätäkseen uuden laitteen käyttöön, käyttäjän tulee käyttää IP-kameran käyttäjätiliä, josta löytyvät kaikki muutkin lisätyt kameralaitteet, jotka voivat olla liitettynä kameraan. Ensimmäistä yhdistämiskertaa varten kamera tarvitsee langattoman lähiverkon verkkotunnuksen (SSID) ja Wi-Fi:n salasanan. Tämä tieto lähetetään suoraan mobiilisovelluksesta kameralle. Jokaiselle uudelle kameralaitteelle annetaan uusi salasana siinä yhteydessä, kun se ensimmäistä kertaa lisätään IP-kameran käyttäjätiliin. Mobiilisovelluksen taustalla toimiva palvelin tunnistaa käyttäjätiliin liitetyt kamerat niille aikaisemmin annetun salasanan perusteella.

Tietoturvariskien perusteellista analysointia varten Seralathan ja muut [2018] suorittivat kameralle verkko- ja sovelluksen tietoturva-analyysin. Verkkotietojen talteenottovaiheen aikana Seralathan ja muut [2018] havaitsivat, että kaikki tiedot siirtyivät puhtaana tekstinä. Tämä tarkoittaa sitä, että kaikki data, jota tiedonsiirrossa liikku IP-kameran, mobiilisovelluksen ja palvelimen välillä on suoraan luettavassa muodossa. Laitteessa ei käytetty minkäänlaista salaustekniikkaa viestintää varten, joten mitään viestintää ei salattu, jota liikkui kameran, palvelimen ja sovelluksen välillä. Esimerkiksi kaikki käyttäjätilin tiedot lähetetään puhtaana tekstinä, kuten myös kameran id sekä salasana, joka alun perin on asetettu kameraan tunnistautumista varten. Tämä luonnollisesti tarkoittaa sitä, että kyseiset kamerat ovat todella alttiitta tietoturvariskeille.

4 IoT:n protokollat, standardit ja kerrokset

Tässä luvussa esitellään erilaisia protokollia ja standardeja, joita IoT-laitteisiin liittyy. Tämän lisäksi tässä luvussa kuvataan kolme pääsiallista kerrosta, jotka IoT:ssa vaikuttavat. Luku on melko tekninen ja sisältää paljon teknistä sanastoa. Oleellisimpia termejä on pyritty määrittelemään alapuolella löytyvään taulukkoon. Osa termeistä on myös sellaisia, että ne esiintyvät muissakin luvuissa. Tämän luvun tarkoituksena on pohjustaa lukua 5, jossa käsitellään IoT:hen liittyviä tietoturvavaatimuksia yleisellä tasolla sekä erityisesti lukua 6, jossa käsitellään yksityiskohtaisemmin IoT:n tietoturvaongelmia.

Termi	**Selite**
Asynkroninen viestinvälitys (Asynchronous messaging)	Viestintämenetelmä, jossa lähetettävä osapuoli voi lähettää viestin ja jatkaa tehtäviään odottamatta välitöntä vastausta toiselta osapuolelta. [Abeykoon, 2019].
Gateway (yhdyskäytävä)	Yhdyskäytävä on tietoliikenteessä käytetty verkkosolmu, joka yhdistää kaksi verkkoa, joilla on erilaiset lähetysprotokollat. Yhdyskäytävät toimivat verkon tulo- ja poistumispisteinä, koska kaiken tiedon on kuljettava yhdyskäytävän läpi tai kommunikoitava sen kanssa ennen reititystä. [Rouse. F.]
HTTP (HyperText Transfer Protocol)	HTTP on taustalla oleva Internet-verkon käyttämä protokolla, ja tämä protokolla määrittelee viestien muotoilun ja lähettämisen sekä web-palvelimien ja selainten toimenpiteiden vastauksena erilaisiin komentoihin. [Beal].
ICMP (Internet Control Message Protocol)	Protokolla, jota verkkolaitteet (esim. reitittimet) käyttävät virheviestien tuottamiseen. [Cooper, 2019].
IEEE (Institute of Electrical and Electronic Engineers)	IEEE on ammattiyhdistys, joka kehittää, määrittelee ja tarkistaa elektroniikan ja tietotekniikan standardeja. [TechTerms, 2015].
IEEE 802.15.4	IEEE:n standardi, joka on suunniteltu alhaisen nopeuden omaaville henkilökohtaisille langattomille verkoille. [Lee, 2004].
IPv6 (Internet Protocol Version 6)	Uusin versio Internet-protokollasta, joka tunnistaa laitteita mahdollistaen niiden paikantamisen. [Shaw, 2018].
Langaton sensoriverkko (WSN)	Langaton sensoriverkko on ryhmä erikoistuneita muuntimia, jotka tarkkailevat ja tallentavat olosuhteita eri paikoissa. Yleisesti tarkkailtavia asioita ovat lämpötila, kosteus, paine, nopeus, äänen voimakkuus ja voimajohdon jännite. [Rouse, E.]
Link Layer (linkkikerros)	Ohjelman protokollakerros verkossa, joka käsittelee datan siirtämistä fyysiseen linkkiin ja sieltä pois. [Rouse, D].
LoRaWAN (Long Range Wide Area Network)	MAC kerrokseen liittyvä protokolla, joka on suunniteltu yhden operaattorin suurille julkisille verkoille. [Schatz, 2016].
LPWAN (Low Power Wide Area Network)	LPWAN-ratkaisuja käytetään IoT:ssa sellaisissa tapauksissa, joissa laitteiden on lähetettävä pieniä määriä dataa säännöllisesti etäverkoissa, jotka kattavat suuria alueita ja akkukäyttöisiä laitteita, joiden on kestettävä useita vuosia. [Wedd, 2018].
LR-WPAN (Low-Rate Wireless Personal Area Network)	Tarkoittaa alhaisen nopeuden henkilökohtaista langatonta verkkoa. [Zheng ja Lee 2004].

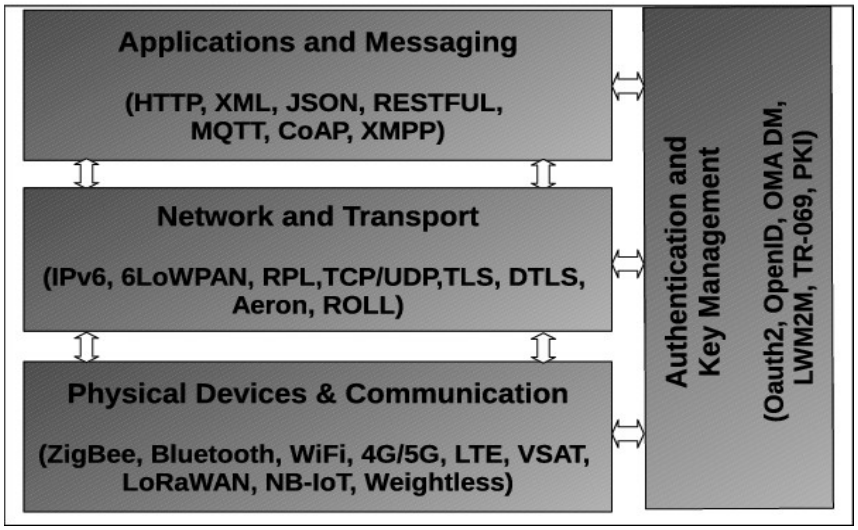
LTE (Long Term Evolution)	Langattoman 4G-laajakaistateknologian standardi, joka tarjoaa suurempaa verkon kapasiteettia ja nopeutta mobiililaitteiden käyttäjille. [Rouse, H].
MAC (Media Access Control)	Säännös tiedonsiirtoa varten, joka määrittelee, kuinka data siirretään kahden tietokonepäätteen välillä. [Mehl, 2019].
MTU (Maximum Transmission Unit)	MTU, eli enimmäislähetysyksikkö on suurin paketin koko, jota voidaan lähettää verkoissa, kuten Internetissä. [Cohen, 2017].
Naapurin löytäminen (Neighbor discovery)	Naapurin löytäminen ratkaisee joukon ongelmia, jotka liittyvät solmujen väliseen vuorovaikutukseen, jotka ovat kiinnitettynä samaan linkkiin. [Walls, 2012].
NB-IoT (kapeakaistainen Internet)	3GPP:n standardoima radiolähetystekniikka langatonta viestintää varten. Se sopii erityisen hyvin suurille määrille yksinkertaisia laitteita. [Kuhlins ja Törnqvist 2019.]
Point-to-Point	Käytetään pääasiallisesti kahden sijainnin välisessä kommunikaatiossa, jossa lähetetään luottamuksellista dataa. [Goines, 2018].
RPL (Routing Protocol)	Reititysprotokolla pienitehoisille ja häviöllisille verkoille. [Khan ja Khaled 2017].
Sensor node (Anturisolmu)	Verkossa on useita ilmaisimia, joita kutsutaan anturisolmuiksi, jotka ovat pieniä, kevyitä ja kannettavia. Jokainen anturisolmu on varustettu anturilla, mikrotietokoneella, lähettimellä, vastaanottimella ja virtalähteellä. [Rouse, E.]
Solmu (Node)	Solmu on mikä tahansa fyysinen laite, joka pystyy lähettämään, vastaanottamaan tai välittämään dataa. Tietokone on yleisin solmu. [Fisher, 2019].
Sybil	Sybil-hyökkäyksessä hyökkääjä osallistuu verkkoon useilla väärennetyillä identiteeteillä, jonka tarkoituksena on heikentää verkon perustavanlaatuisten toimintojen toimintaa. Näitä väärennettyjä identiteettejä kutsutaan Sybil-solmuiksi. [Vasudeva ja Sood 2018.]
Tavoittamaton kohde (Destination unreachable)	On olemassa monia mahdollisia syitä siihen, että kohdeisäntää ei tavoitettu, jotka puolestaan johtavat ”Destination host unreachable” -virheisiin. Yksinkertaiset asiat kuin virheellisesti kytketyt kaapelit tai palomuuri voivat aiheuttaa oheisia virheitä. [Wilton, 2019.]
TCP (Transmission Control Protocol)	TCP on standardi, joka määrittelee, miten perustetaan ja ylläpidetään verkkokeskustelua, jonka kautta sovellusohjelmat voivat vaihtaa dataa keskenään. [Rouse, A].
UDP (User Datagram Protocol)	UDP on vaihtoehtoinen tiedonsiirtoprotokolla TCP:lle, jota käytetään ensisijaisesti alhaisen viiveen ja häviämistä sietävien yhteyksien luomiseen Internet-sovellusten välillä. [Rouse, B].
WAN (Wide Area Network)	WAN eli laajakaistaverkko on maantieteellisesti hajautettu yksityinen televerkko, joka yhdistää useita lähiverkkoja (LAN). [Rouse, C].
Weightless Protocol (Painoton protokolla)	Avoin standardi / protokolla IoT-viestintäverkoille, jonka on kehittänyt ja koordinoinut voittoa tavoittelematon ryhmä, Weightless Special Interest Group (SIG). Painoton tarjoaa kolme standardia tukemaan erilaisia IoT-käyttötapauksia. [McHoul, 2017.]
Ylätunnisteiden kompressio (Header compression)	Ylätunnisteiden kompressio on mekanismi, joka pakkaa paketin IP-otsakkeen ennen paketin lähettämistä. [Cisco, 2018].
3GPP (3rd Generation Partnership Project)	On teleyritysten yhteistyöhanke, jonka lähtökohtana on kehittää maailmanlaajuisesti sovellettavia eritelmiä kolmannen sukupolven matkaviestijärjestelmille (3G). [Rouse, G].

6LoWPAN (IPv6 over Low power Wireless Area Networks)	Mahdollistaa kooltaan pienempien ja prosessointiteholtaan heikkojen laitteiden tiedon siirtämisen langattomasti. [Ray, 201].

Taulukko 1. Oleellisten termien määritykset liittyen lukuihin 4, 5 ja 6.

4.1 Protokollista ja standardeista

Kuva 3 esittää kerrostettua arkkitehtuuria ja yleisiä IoT protokollia, jotka liittyvät sovelluksiin ja viestintään, reititykseen/edelleen lähettämiseen, autentikointiin, avainten hallintaan ja fyysisiin laitteisiin. Se sisältää myös standardit sekä protokollat yleisesti käytetyille alhaisen nopeuden henkilökohtaisille langattomille verkoille (LR-WPAN) ja hiljattain kehitetyt protokollat pienitehoisille laajakaistaverkoille (LPWAN). [Khan ja Khaled 2017.]



Kuva 3 Yleiset IoT standardit ja protokollat. [Khan ja Khaled 2017: 397].

LR-WPAN-laitteille IEEE-standardi 802.15.4 kuvaa kahta matalatason kerrosta: fyysistä kerrosta ja keskitason pääsynhallintaa, eli MAC (Medium Access Control) -kerrosta. Fyysisen kerroksen määrittely liittyy viestintään langattomien kanavien kautta, joilla on erilaisia taajuuskaistoja ja datanopeuksia. MAC-kerrosmäärittely liittyy kanavakäytön ja synkronoinnin mekanismeihin. IEEE 802.15.4:n standardissa käytetään enimmäislähetysyksikköä (MTU), joka on pienikokoinen. Enimmäislähetysyksikön pieni koko mahdollistaa sen, että mukautuskerros voidaan sisällyttää pienitehoisille langattomille henkilökohtaisille verkoille (6LoWPAN) käyttäen IPv6:ta. Mukautuskerros sisällytetään linkkikerroksen (link layer) yläpuolelle parantamaan anturisolmun (sensor node) IP-pohjaisen viestinnän valmiuksia. Jokainen IoT-laite tunnistetaan yksilöllisesti

IPv6 verkko-osoitteella. Pienitehoisille ja häviöllisille verkoille (low-power lossy networks) käytetään reititysprotokollaa, joka auttaa tukemaan 6LoWPAN-ympäristöjen toimintaa. RPL-standardi tukee sekä pisteeltä pisteelle -liikennettä (Point-to-Point) että viestintää monen (multipoint communication) ja yhden pisteen (single point communication) välillä. [Khan ja Khaled 2017.]

Rajoitetun hyötykuormansa vuoksi IoT:n sovellussuunnittelu käyttää UDP:ta (User Datagram Protocol) viestintää varten, koska se on tehokkaampi ja vähemmän monimutkaisempi kuin TCP (Transmission Control Protocol). Lisäksi UDP:n ylätunnisteiden kompressio (header compression) voidaan suorittaa tehokkaammin rajoitettua hyötykuormatilaa varten. Ohjausviestejä (control messages) käytetään 6LoWPAN:ssa tavoittamattoman kohteen (Destination unreachable) määrittelyssä ja naapurien löytämisessä (Neighbor Discovery). Ohjausviestien tukena käytetään ICMP:tä (Internet Control Message Protocol). Rajoitettu sovellusprotokolla (CoAP) tarjoaa pyyntö-vastauspohjaisen (request-response) mallin pienitehoisille ja häviöllisille verkoille, jotka toimivat rajoitetuissa ympäristöissä. CoAP-protokolla tukee asynkronista viestintävälitystä (asynchronous message communication) ja se tarjoaa myös HTTP:n määrittelyä saadakseen pääsyn IoT resursseihin HTTP:n kautta. [Khan ja Khaled 2017.]

LPWAN mahdollistaa pitkän kantaman kommunikoinnin laitteille IoT-verkoissa. Toisin kuin langaton WAN, joka vaatii enemmän virtaa työskennelläkseen suurella bittinopeudella (bit-rate), se tukee pienitehoista tiedonsiirtoa alhaisella bittinopeudella. LPWAN käyttää LoRaWAN-protokollaa yhdyskäytävien (gateway) ja päätelaitteiden kommunikointia varten, samalla tukien vaihtelevaa tiedonsiirtonopeutta akkukäyttöisten laitteiden verkossa. Samoin myös kapeakaistainen Internet (NB-IoT) on 3GPP-protkolla LPWAN kommunikointiin, joka tarjoaa näkyvyyttä sisätiloissa (indoor coverage) samalla, kun käytetään LTE:tä. Painoton protokolla (The Weightless protocol) käyttää LPWAN-tiedonsiirrossa kolmea erilaista standardia tukemaan vastaavasti yksisuuntaista, kaksisuuntaista ja vähän virtaa käyttävää tilaa. [Khan ja Khaled 2017.]

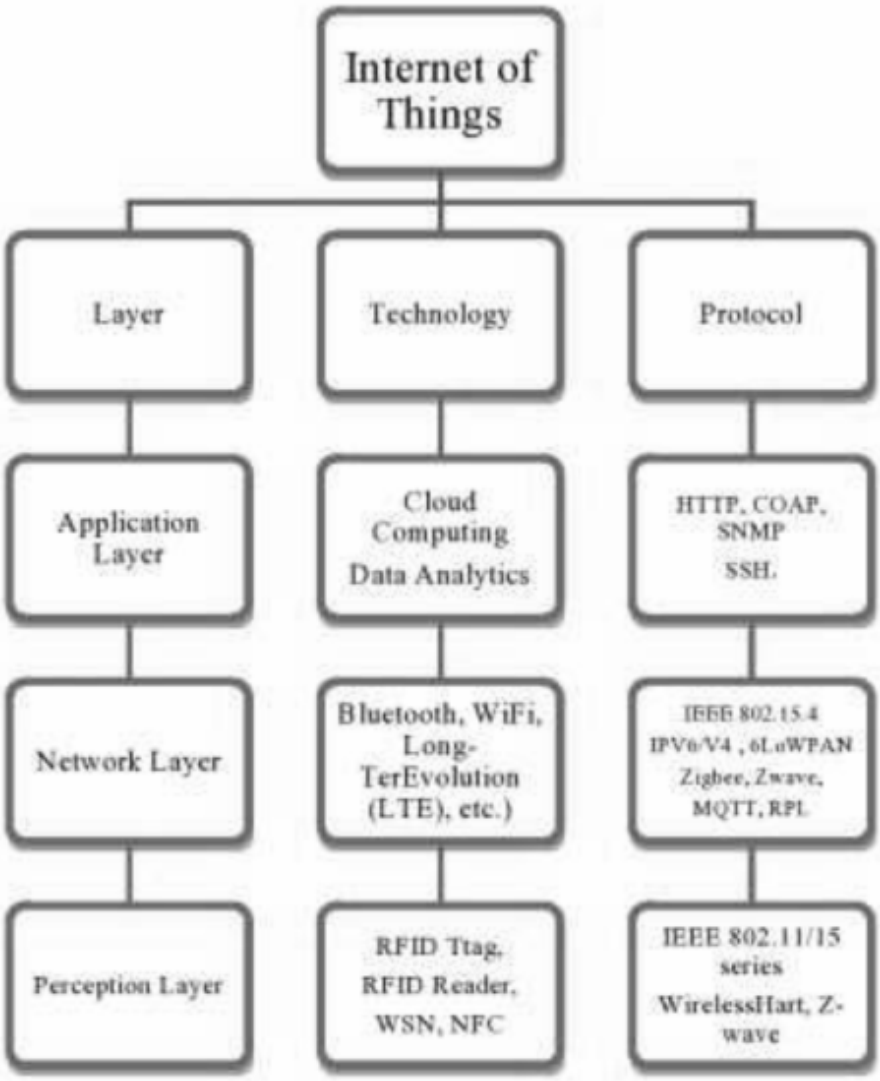
4.2 IoT:n kerrokset

IoT:hen liittyy kolme eri kerrosta, joista alin taso on havaintokerros (Perception layer). Havaintokerros kerää kaiken tyyppisiä tietoja fyysisten laitteiden ja niiden sensorien, kuten GPS:n kautta. Tämän kerroksen avainkomponenttina toimii anturi, joka kerää ja esittää tietoja fyysisestä maailmasta digitaaliseen maailmaan. Tämän kerroksen aistivilla solmuilla on yleensä rajoitettu teho ja tallennuskapasiteetti, joka tekee

tietosuojajärjestelmän perustamisesta erittäin haastavaa. Samaan aikaan ulkopuoliset hyökkäykset, kuten palvelunestohyökkäykset aiheuttavat jatkuvasti uusia tietoturvaongelmia. Tässä kerroksessa sensoreihin liittyvä data tarvitsee suojausta taatakseen niiden eheyden ja aitouden. [Abdullah et al., 2019.]

Tietoverkkokerros (Network layer) on toinen kerros, jonka pääroolina on luotettavan tiedonsiirron, eli synkronoinnin toteuttaminen havaintokerroksesta. Tässä kerroksessa tiedonsiirto käyttää perusverkkoja. Perusverkkoja ovat esimerkiksi mobiili, yksityinen, langaton ja langallinen verkko. Viestintäprotokollat ovat myös tärkeitä laitteiden välisessä tiedonvaihtoprosessissa tässä kerroksessa. Verkkokerros koostuu langattomasta sensoriverkosta (WSN), joka vastaa datan siirtämisestä anturista tarkoitettuun määränpäähän erittäin luotettavasti. Verkkokerroksella on suhteellisen korkea kyky tarjota lähes täydellistä tietoturvaa, mutta hyökkäykset, kuten väärennöshyökkäykset (Counterfeit attack) ovat kuitenkin mahdollisia. Verkon ruuhkat ovat myös mahdollisia, mikäli virtaavan datan määrä on erittäin suuri. Siksi tämän kerroksen turvallisuusmekanismit ovat erittäin tärkeitä IoT:lle. [Abdullah et al., 2019.]

Sovelluskerros (Application layer) on ylin kerros, joka tarjoaa henkilökohtaisia palveluita käyttäjien tarpeiden mukaan. Sovelluskerroksen käyttöliittymä tarjoaa käyttäjille pääsyn Internet-sovelluksiin henkilökohtaisen tietokoneen tai mobiililaitteiden avulla. Suojaustarpeet vaihtelevat eri sovellusympäristöissä, ja etenkin tiedonjako-ominaisuus aiheuttaa monia ongelmia liittyen tietosuojaan, pääsynvalvontaan ja tietojenkäsittelyyn. [Abdullah et al., 2019.]



Kuva 3. IoT:n kerrokset ja niihin liittyviä teknologioita ja protokollia. [Kamble ja Bhutad 2018: 307].

5 Tietoturvavaatimukset

Khan ja Khaled [2017] nostavat esille useita huomioita ja vaatimuksia, joita turvallisen sekä vakaan IoT-ympäristön tulisi ottaa huomioon. Nämä huomiot liittyvät tietosuojaan, todentamiseen, palvelujen saatavuuteen, energiatehokkuuteen ja yksittäisen pisteen toimintahäiriöihin.

Koska kaikki IoT-data kulkee verkon välityksellä, ovat asianmukaiset salausmekanismit tarpeen, jotta datan luotettavuus voidaan varmistaa. Palvelujen, laitteiden ja verkon monimuotoisen integroinnin takia laitteisiin tallennetut tiedot ovat alttiita yksityisyyden loukkauksille, jos IoT-verkossa olevien solmujen tietoturva pääsee vaarantumaan. Ulkopuoliset hyökkääjät pystyvät vaikuttamaan altistuneen IoT-laitteen

tallennettujen tietojen eheyteen tai muuttamaan niitä muuten haitallisiin tarkoituksiin. [Khan ja Khaled 2017.]

Turvallisen tietoliikenteen turvaamiseksi IoT:ssa tarvitaan todennus (authentication) kahden osapuolen välillä, jotka kommunikoivat keskenään. Etuoikeutettua yhteyttä (privileged access) varten, laitteiden on oltava todennettuja. IoT:n monimuotoiset todennusmekanismit ovat lähinnä olemassa siksi, koska IoT-laitteiden taustalla toimii moninaisia heterogeenisiä ympäristöjä ja arkkitehtuureita, jotka tukevat niitä. Nämä ympäristöt aiheuttavat haasteita standardoidun globaalin protokollan määrittämiselle todennusta varten IoT:ssa. Samoin myös valtuutusmekanismit varmistavat, että pääsy järjestelmiin tai tietoihin tarjotaan valtuutetuille (authorization). Valtuutus- ja todennustulosten asianmukainen toteutus takaavat luotettavan ympäristön, jossa kommunikaatio on turvallisia. Lisäksi resurssien käytön kirjanpito sekä tarkastus ja raportointi tarjoavat luotettavan mekanismin verkonhallinnan turvaamiseksi. [Khan ja Khaled 2017.]

IoT-laitteisiin kohdistuvat hyökkäykset voivat haitata palvelujen tarjoamista tavanomaisten palvelunestohyökkäysten (Denial of service attack) kautta. Myös erilaisia strategioita, kuten syvennyshyökkäyksiä (Sinkhole attack), vastapuolen häirintää (Jamming adversaries) tai uusintahyökkäyksiä (Replay attack) käytetään hyväksi IoT-komponenttien häiritsemisessä eri tasoilla samalla huonontaen tarjotun palvelun laatua IoT:n käyttäjille. [Khan ja Khaled 2017.]

IoT-laitteet ovat tyypillisesti resurssirajoitettuja. Tämä tarkoittaa käytännössä sitä, että niille on ominaista vähäinen virrankäyttö ja pieni tallennustilan määrä. IoT:n arkkitehtuuriin kohdistuvat hyökkäykset voivat johtaa kasvaneeseen energiankulutukseen tukkimalla verkkoliikenteen ja kuluttamalla IoT:n resurssit loppuun tarpeettomilla tai väärennetyillä palvelupyynnöillä. [Khan ja Khaled 2017.]

IoT-pohjaisen infrastruktuurin heterogeenisten verkkojen jatkuva kasvu voi paljastaa suuren määrän yksittäisiä virhepisteitä, mikä puolestaan voi huonontaa IoT:n kautta suunniteltuja palveluita. Se edellyttää väärentämisen estävän ympäristön kehittämistä suurelle määrälle IoT-laitteita sekä vaihtoehtoisten mekanismien tarjoamisen vikasietoisten verkkojen toteuttamiseksi. [Khan ja Khaled 2017.]

6 Tietoturvaongelmien esittely

Khan ja Khaled [2017] jakavat IoT:hen liittyviä tietoturvaongelmia kolmeen eri kategoriaan: Alhaisen tason, keskitason ja korkean tason tietoturvaongelmiin. Khan ja

Khaled [2017] linjaavat alhaisen tason ongelmien liittyvän laitteiston rautatasoon ja fyysiseen puoleen sekä linkkikerroksen kommunikointiin. Keskitason ongelmat liittyvät heidän mukaansa enimmäkseen kommunikointiin, reititykseen ja verkkotasoon. Puolestaan korkean tason ongelmiksi he nostavat ne, jotka liittyvät sovellustasolle. Tämän lisäksi Kamble ja Bhutad [2018] erittelevät tietoturvaongelmia sen mukaan, mihin kerrokseen kyseinen ongelma liittyy. Nämä kerrokset ovat esitelty luvussa 4 ja ne ovat: Havaintokerros, tietoverkkokerros ja sovelluskerros.

Riippuen lähteestä, IoT-laitteiden tietoturvaongelmia esitellään hieman eri tavoilla. Esimerkiksi Khanin ja Khaledin [2017] käyttämä esitystapa poikkeaa verrattaessa Kamblen ja Bhutadin [2018] käyttämään esiystapaan. Pääosin kuitenkin Khanin ja Khaledin [2017] tasot vastaavat Kamblen ja Bhutadin [2018] esittelemiä kerroksia (alhainen taso = havaintokerros, keskitaso = tietoverkkokerros ja korkea taso = sovelluskerros), mutta näissä on hieman poikkeuksia. Esimerkiksi Khanin ja Khaledin [2017] alhainen taso vastaa suurilta osin havaintokerrosta, mutta siitä löytyy myös jonkin verran viitteitä tietoverkkokerrokseen. Tässä kappaleessa olevia ongelmia esitellään käyttäen kumpaakin ylempänä esiteltyä luokittelumallia ja siitä syystä esimerkiksi jokin Khanin ja Khaledin [2017] alhaiseen tasoon liitetty ongelma saattaakin liittyä Kamblen ja Bhutadin [2018] mukaan tietoverkkokerrokseen. Jotkin ongelmat ovat puolestaan esitelty vain käyttäen toista ylempänä esitellyistä luokittelumalleista. Tämä siitä syystä, sillä Khan ja Khaled [2017] eivät esimerkiksi erikseen luokittele palvelunestohyökkäyksiä, jotka ovat kuitenkin eräitä yleisimpiä tietoturvaongelmia. Samoin on myös ongelmia, joita Kamble ja Bhutan [2018] eivät erikseen luokittele, mutta niitä olisi syytä esitellä. Seuraavassa luvussa esiteltyjä ongelmia on pyritty valitsemaan siten, että jokaisesta aikaisemmin esitellystä kerroksesta / tasosta on tuotu esille vähintään muutama tietoturvaongelma. Ongelmien valitsemiseen on myös vaikuttanut erityisesti se, että ne ovat nostettu molemmissa (Khan ja Khaled [2017] ja Kamble ja Bhutad [2018]) teksteissä vahvasti esille.

Ongelmat esitellään nimeltä ja niihin on kiinnitetty vaikuttava taso / kerros, johon ongelma liittyy. Tässä on listattu molemmat (Khan ja Khaled [2017] ja Kamble ja Bhutad [2018]), jos ongelma löytyy kummastakin lähteestä. Jos se löytyy vain toisesta, on tähän sarakkeeseen listattu esimerkiksi vain ” [Khan ja Khaled 2017]”. Jokainen ongelma on kuvattu selitteellä ja selite on valittu aina vain yhdestä työstä, esimerkiksi ” [Kamble ja Bhutad 2018.]”.

Vastapuolen häirintä (Jamming adversaries)

- **Vaikuttava taso / kerros:** Alhainen taso [Khan ja Khaled 2017].
- **Selite:** IoT:n langattomien laitteiden häirintähyökkäysten tarkoituksena on heikentää verkkojen toimintaa IoT:ssa, jota toteutetaan lähettämällä verkossa radion taajuussignaaleja, jotka eivät noudata mitään määriteltyä protokollaa. Tämä häirintä voi vaikuttaa vakavasti verkon toimintaan vaikeuttamalla oikeiden solmujen datan vastaanottamista ja lähettämistä, joka voi johtaa järjestelmän arvaamattomaan toimintaan. [Khan ja Khaled 2017.]

Epävarma alustus (Insecure initialization)

- **Vaikuttava taso / kerros:** Alhainen taso [Khan ja Khaled 2017].
- **Selite:** Turvalliset mekanismit IoT:n alustamiseen ja konfigurointiin varmistavat asianmukaisen toiminnan koko järjestelmässä ilman yksityisyyden loukkauksia ja haitallisia vaikutuksia verkkopalveluihin. Myös fyysisen kerroksen viestintä on varmistettava, jotta sinne ei ole pääsyä luvattomille vastaanottimille. Edellä mainittujen esimerkkien epävarma alustus voi johtaa siihen, että luvattomat vastaanottimet pääsevät käsiksi fyysiseen kerrokseen. [Khan ja Khaled 2017].

Alhaisen tason Sybil- ja huijaushyökkäykset

- **Vaikuttava taso / kerros:** Tietoverkkokerros [Kamble ja Bhutad 2018] ja alhainen taso [Khan ja Khaled 2017].
- **Selite:** Sybil-hyökkäykset langattomassa verkossa johtuvat haitallisista Sybil-solmuista, jotka käyttävät vääriä identiteettejä heikentääkseen IoT:n toimivuutta. Alhaisella tasolla Sybil-solmu voi käyttää satunnaisesti väärennettyjä MAC-arvoja maskeeraukseen itsensä toiseksi laitteeksi, jonka tarkoitus on ehdyttää verkon resursseja. Tämä voi johtaa siihen, etteivät oikeat solmut pääse verkon resursseihin käsiksi. [Khan ja Khaled 2017].

Väärien tietojen syöttöhyökkäykset (False Data Injection Attacks)

- **Vaikuttava taso / kerros:** Havaintokerros [Kamble ja Bhutad 2018].
- **Selite:** Väärien tietojen syöttöhyökkäyksissä käytetään siepattuja solmuja tai laitteita lähettämään vääriä tietoja IoT-sovelluksille. Saatuaan vääriä tietoja, IoT-sovellusten toiminta voi muuttua epävarmaksi ja ne voivat esimerkiksi lähettää

virheellisiä ilmoituksia, tarjota vääriä ohjeita tai tarjouksia. Tämä voi puolestaan johtaa koko verkon heikentyneen toimintaan. [Kamble ja Bhutad 2018.]

Epäturvalliset fyysiset käyttöliittymät ja rajapinnat

- **Vaikuttava taso / kerros:** Alhainen taso [Khan ja Khaled 2017].
- **Selite:** Useat fyysiset tekijät aiheuttavat vakavia uhkia laitteiden asianmukaiselle toiminnalle IoT:ssa. Huono fyysinen suojaus, ohjelmistojen käyttö fyysisten rajapintojen kautta ja testaukseen tai virheenkorjaukseen käytettyjä työkaluja voidaan hyödyntää solmujen altistamiseksi verkossa [Khan ja Khaled 2017].

Unen puute -hyökkäykset (Sleep deprivation attack)

- **Vaikuttava taso / kerros:** Tietoverkkokerros [Kamble ja Bhutad 2018] ja alhainen taso [Khan ja Khaled 2017].
- **Selite:** Energiarajoitetut laitteet IoT:ssa ovat alttiita unen puute -hyökkäyksille. Tällä tarkoitetaan sitä, että IoT:ssa olevat anturisolmut pakotetaan pysymään hereillä, eivätkä ne pääse lepäämään. Toisin sanoen näiden hyökkäysten tarkoitus on kuluttaa laitteessa oleva akku loppuun pakottamalla laitteen tekemään suuri määrä tehtäviä 6LoWPAN ympäristössä. [Khan ja Khaled 2017.]

Palvelunestohyökkäykset (Denial of service attack)

- **Vaikuttava taso / kerros:** Tietoverkkokerros [Kamble ja Bhutad 2018].
- **Selite:** Palvelunestohyökkäykset ovat hyökkäyksen muoto, jossa verkkoa kuormitetaan suurella tietoliikenteen määrällä, joka johtaa järjestelmän hyödyllisten resurssien tyrehtymiseen. Tämä voi puolestaan johtaa siihen, ettei laite tai verkko ole oikeiden käyttäjien käytettävissä. Palvelunestohyökkäyksiä voidaan tuottaa järjestelmällisesti erilaisten hyökkäysjärjestelmien kautta. IoT:n turvaamiseksi on kehitettävä järjestelmiä, jotka voivat lieventää palvelunestohyökkäyksiä ja niiden vaikutuksia. [Kamble ja Bhutad 2018.]

Syvennys ja madonreikä -hyökkäykset (Sinkhole and wormhole attacks)

- **Vaikuttava taso / kerros:** Tietoverkkokerros [Kamble ja Bhutad 2018] ja keskitaso [Khan ja Khaled 2017].
- **Selite:** Vajoamahyökkäyksissä hyökkäävä solmu vastaa reitityspyyntöihin, jolloin paketit kulkevat hyökkäävän solmun läpi, jota puolestaan voidaan käyttää

haitallisten toimintojen suorittamiseen verkossa. Verkkoa vastaan kohdistuvat hyökkäykset voivat entisestään heikentää 6LoWPAN:in toimintaa myös madonreikähyökkäysten toimesta. Madonreikähyökkäyksessä tehdään tunneli kahden solmun välille niin, että solmuun saapuvat paketit saavuttavat myös toisen solmun välittömästi. Näillä hyökkäyksillä on vakavia vaikutuksia mukaan lukien salakuuntelu, yksityisyyden loukkaukset, vakoilu ja palvelunesto. [Khan ja Khaled 2017.]

RPL -reitityshyökkäykset (RPL routing attack)

- **Vaikuttava taso / kerros:** Keskitaso [Khan ja Khaled 2017].
- **Selite:** IPv6 reititysprotokolla pienitehoisille ja häviöllisille verkoille (RPL) on altis useille hyökkäyksille verkossa olevien vaarantuneiden solmujen kautta. Hyökkäykset voivat johtaa resurssien tyrehtymiseen ja salakuunteluun. [Khan ja Khaled 2017.]

Epäturvalliset rajapinnat

- **Vaikuttava taso / kerros:** Korkea taso [Khan ja Khaled 2017].
- **Selite:** IoT:n palveluihin pääsyä varten käytetyt verkko, mobiili -ja pilvipalveluiden rajapinnat voivat altistaa IoT:n monille erilaisille hyökkäyksille. Nämä hyökkäykset voivat vaikuttaa vakavasti tietosuojaan ja yksityisyyteen. [Khan ja Khaled 2017.]

Epäturvalliset ohjelmistot/haittaohjelmat

- **Vaikuttava taso / kerros:** Sovelluskerros [Kamble ja Bhutad 2018] ja korkea taso [Khan ja Khaled 2017].
- **Selite:** Haittaohjelmat, kuten virukset voivat saastuttaa IoT-sovelluksia. Saastuneet tai muuten epäturvalliset ohjelmat voivat altistaa IoT:n käyttäjän yksityisyyden vaaraan, sillä haittaohjelmien tarkoituksena on usein päästä käsiksi käyttäjän yksityiseen dataan, joka puolestaan vaarantaa tietosuojan. [Kamble ja Bhutad 2018.]

Verkkourkinta / tietojenkalastelu (Phising)

- **Vaikuttava taso / kerros:** Sovelluskerros [Kamble ja Bhutad 2018].

- **Selite:** Tietojenkalasteluhyökkäyksissä on tarkoituksena saada IoT:n käyttäjiltä yksityistietoja, kuten käyttäjätietoja, henkilöllisyystietoja tai salasanoja erilaisin huijausmenetelmin. Nämä huijausmenetelmät voivat vaihdella saastuneista sähköposteista erilaisiin verkkosivustoihin, joilla käyttäjää pyydetään syöttämään todennustietoja. [Kamble ja Bhutad 2018.]

7 Yhteenveto

Tämän kandidaattityön tarkoituksena on ollut perehtyä siihen, minkälaisessa tilassa IoT-laitteiden tietoturva on ja ensi kädessä tutkia sitä, minkälaisia tietoturvaongelmia IoT-laitteisiin mahdollisesti liittyy. Yleisenä havaintona IoT-laitteista voidaan nostaa esille sen, että niiden määrä on kasvanut nopeasti ja kuten luvussa kaksi on nostettu esille, IoT:n määritelmä ei ole täysin yksiselitteinen. Käytännössä mikä tahansa elektroninen tai akkukäyttöinen laite voidaan luokitella IoT-laitteeksi, jos se kykenee yhdistymään verkkoon ja sitä kautta toisiin laitteisiin. Tässä työssä kuitenkin havaittiin, että IoT:n nopeasta kasvusta huolimatta kasvu olisi voinut olla entistäkin nopeampaa ja tähän merkittävänä syynä ovat vaikuttaneet IoT-laitteita vaivaavat tietoturvaongelmat.

Tässä työssä tehtiin aluksi katsaus siihen, mitä IoT yleisesti tarkoittaa, miten se toimii ja minkälaisia IoT-laitteita voi olla olemassa. Tämän lisäksi oli määritettävä se, mitä tarkoittavat tietototurva sekä tietosuoja ja lisäksi oli nostettava esille tietoturvan erot verrattaessa kyberturvallisuuteen. Seuraavaksi tarkasteltiin IoT-laitteiden tietoturvaa yleisellä tasolla ja nostettiin esille syitä siihen, miksi ylipäätänsä kuluttajamarkkinoille on päässyt paljon sellaisia laitteita, joiden tietoturva on heikolla tasolla. Tässä olennaisena syynä havaittiin, että monet yritykset julkaisivat taloudellisten voittojen toivossa käytännössä keskeneräisiä laitteita markkinoille, joiden tietoturva ei ollut riittävä. Tämän lisäksi nostettiin esille esimerkkien avulla huomioita siitä, miten tietoturvaongelmat voivat käytännössä näkyä IoT:n käyttäjille.

Neljännessä ja viidennessä luvussa käsiteltiin IoT:hen liittyviä protokollia, standardeja ja yleisiä tietoturvavaatimuksia sekä sitä, minkälainen arkkitehtuuri IoT:lla on. Havaittiin, että IoT rakentuu käytännössä kolmesta eri kerroksesta: Havaintokerros, tietoverkkokerros ja sovelluskerros. Näissä luvuissa esiteltyjä protokollia, standardeja ja kerroksia hyödynnettiin kuudennen luvun varsinaisten tietoturvaongelmien esittelyssä.

Kuudennessa luvussa esiteltiin yksityiskohtaisemmin varsinaisia tietoturvaongelmia, joita IoT-laitteissa esiintyy. Esiteltyjä tietoturvaongelmia pyrittiin esittelemään sen mukaan, missä yllä mainituista IoT:n kerroksista tietoturvaongelma vaikuttaa. Esitetyt

tietoturvaongelmat valittiin enimmäkseen sen perusteella, esiintyikö kuvattu ongelma kummassakin käytetyistä lähteistä. Tämän lisäksi käytetyissä lähteissä oli hieman eroavaisuuksia siinä, mihin IoT:n kerrokseen kuvattu tietoturvaongelma liitettiin, jonka takia tietoturvaongelma esittelyn yhteydessä merkattiin kummassakin lähteessä kuvattu IoT-taso tai kerros. Käytetty tietoturvaongelmien esitystapa onnistui kohtalaisen hyvin, mutta siinä olisi voinut olla parantamisen varaa huomioiden luettavuuden ja selkeyden.

Tämän kandidaatintyön perimmäisenä tavoitteena oli löytää, minkälaisia tietoturvaongelmia IoT-laitteista löytyy ja myös käsitellä sitä, miten ne voisivat käytännössä näkyä. Ensimmäinen tavoite täyttyi, sillä erilaisia tietoturvaongelmia löytyi ja paljon. Niiden määrä oli myös niin suuri, että niitä jouduttiin karsimaan ja valitsemaan esiteltäväksi yllä mainittujen perusteiden mukaisesti. Positiivista oli myös se, että käytetyissä lähteissä nostettiin esille paljon samoja tietoturvaongelmia. Jälkimmäinen tavoite vain täyttyi osittain, sillä luvussa kolme kyllä käsiteltiin sitä, miten tietoturvaongelmat käytännössä näkyvät, mutta tämä osuus jäi lyhyeksi. Olisin nimittäin halunnut vielä tarkemmin esitellä jokaisen luvussa 6 valitun tietoturvaongelman yhteydessä esimerkin jostakin käytännön tapauksesta, jossa kyseinen ongelma esiintyi. Huomioiden tämän työn tekstisisällön pituuden, jotakin oli karsittava. Tämän lisäksi työstä jäi myös ulkopuolelle mahdollisten ratkaisujen tai korjausten tarkempi esittely, joilla tietoturvaongelmia voitaisiin kitkeä. Vaikka sitä ei työssä ollutkaan tarkoitus tutkia, heräsi siitä mahdollisia jatkotutkimusajatuksia, joita voisi esimerkiksi gradutyössä jatkaa.

Viiteluettelo

Abdullah, Hamad, Abdulrahman, Moala ja Salim Elkhediri. 2019. CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2019. 1–6.

Abeykoon, Hasitha. 2019. Asynchronous Message-Based Communication. https://wso2.com/library/articles/2019/12/asynchronous-message-based-communication/ (Haettu 23.12.2019).

Adascalitei, Ioan. 2019. Smartphones and IoT Security. *Informatica Economica* 23.2 (2019): 63–75.

Agarwal, Oser, Pascal ja Lueders Stefan. 2019. Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk. *Sensors (Basel, Switzerland)* 19.19 (2019): n. pag.

Alsted, Mathias ja Flinck, Lund. 2018. Mitä EU:n uusi tietosuoja-asetus tarkoittaa? https://kotimikro.fi/tietoturva/tietosuoja/mita-eu-n-uusi-tietosuoja-asetus-tarkoittaa (Haettu 12.1.2019).

Beal, Vangie. HTTP – HyperText Transfer Protocol. https://www.webopedia.com/TERM/H/HTTP.html (Haettu 23.12.2019).

Cisco. 2018. Header Compression Configuration Guide. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_hdrcomp/configuration/xe-16/qos-hdrcomp-xe-16-book/hdr-comp.html (Haettu 23.12.2019).

Clark, Jen. 2016. What is the Internet of Things? https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ (Haettu 12.10.2019).

Cohen, Dor. 2017. MTU and MSS: What you Need to Know https://www.imperva.com/blog/mtu-mss-explained/ (Haettu 15.12.2019).

Cooper, Stephen. 2019. What Is ICMP? https://www.comparitech.com/net-admin/what-is-icmp/ (Haettu 23.12.2019).

Fisher, Tim. 2019. What Is Firmware? https://www.lifewire.com/what-is-firmware-2625881 (Haettu 2.11.2019).

Gilchrist, Alasdair. 2017. *IoT Security Issues.* Boston: Walter de Gruyter, 2017.

Goines, Sean. 2018. Point-to-Point Network. *https://www.telarus.com/resources/solutions/point-to-point-network/* (Haettu 15.12.2019).

Hanes, Salgueiro, Grossetete, Barton ja Jerome, Henry. 2017. *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. N.p.

Hiebert, Lindsay. 2013. Public Safety Blog Series – Connecting the Unconnected in Public Safety Response. https://blogs.cisco.com/government/connecting-the-unconnected-in-public-safety-response (Haettu 12.10.2019).

Kamble, Ashvini ja Bhutad, Sonali. 2018. Survey on Internet of Things (IoT) Security Issues & Solutions. *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. IEEE, 2018. 307–312.

Khan, Minhaj ja Salah, Khaled. 2017. IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Generation Computer Systems* 82 (2018): 395–411.

Kuhlins, Christian ja Törnqvist, Marcus. 2019. What is NB-IoT? Practical tips to unlock its business potential. https://www.ericsson.com/en/blog/2019/10/what-is-NB-IoT (Haettu 12.2019).

Lueth, Knud. 2018. Sate of IoT 2018: Number of IoT devices now at 7b – Market accelerating. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (Haettu 13.10.2019).

McHoul, Dave. 2017. Locating Weightless IoT-Devices. https://www.skyhook.com/blog/iot/location-locating-weightless-devices (Haettu 23.12.2019).

Mehl, Beinhard. 2019. Media Access Control. https://www.getkisi.com/blog/media-access-control (Haettu 15.12.2019).

O'Neill, Maire. 2016. Insecurity by Design: Today's IoT Device Security Problem. *Engineering* 2.1 (2016): 48–49.

Petters, Jeff. 2020. Data Privacy Guide: Definitions, Explanations and Legislation. https://www.varonis.com/blog/data-privacy/ (Haettu 9.2.2020).

Puro, Johannes. 2017. Kuinka ison riskin asioiden internet luo tietoturvan ja kyberturvan kannalta? https://www.itewiki.fi/blog/2017/03/mika-on-tietoturvan-ja-kyberturvallisuuden-ero/ (Haettu 19.10.2019).

Ray, Brian. 2014. 6LoWPAN vs. ZigBee: Two Wireless Technologies Exaplained. https://www.link-labs.com/blog/6lowpan-vs-zigbee (Haettu 15.12.2019).

Rouse, Margaret. A. UDP (User Datagram Protocol). *https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol* (Haettu 23.12.2019).

Rouse, Margaret. B. TCP (Transmission Control Protocl). https://searchnetworking.techtarget.com/definition/TCP (Haettu 23.12.2019).

Rouse, Margaret. C. WAN (Wide Area Network). https://searchnetworking.techtarget.com/definition/WAN-wide-area-network. (Haettu 23.12.2019).

Rouse, Margaret. D. Data-Link layer. https://searchnetworking.techtarget.com/definition/Data-Link-layer. (Haettu 23.12.2019).

Rouse, Margaret. E. Wireless Sensor Network (WSN). https://searchdatacenter.techtarget.com/definition/sensor-network. (Haettu 23.12.2019).

Rouse, Margaret. F. Gateway. https://internetofthingsagenda.techtarget.com/definition/gateway (Haettu 23.12.2019).

Rouse, Margaret. G. 3GPP (3rd Generation Partnership Project). https://searchnetworking.techtarget.com/definition/3rd-Generation-Partnership-Project-3GPP (Haettu 23.12.2019).

Rouse, Margaret. H. LTE (Long Term Evolution). *https://searchmobilecomputing.techtarget.com/definition/Long-Term-Evolution-LTE* (Haettu 23.12.2019).

Schatz, Glenn. 2016. The Complete List Of Wireless Iot Network Protocols. https://www.link-labs.com/blog/complete-list-iot-network-protocols (Haettu 23.12.2019).

Seralathan, Oh, Jadhav, Myers, Jeong, Kim ja Kim, Jeongnyeo. (2018). IoT Security Vulnerability: A Case Study of a Web Camera. *2018 20th International Conference on Advanced Communication Technology (ICACT)*. Global IT Research Institute (GiRI), 2018. 1–2.

Shaw, Keith. 2018. What is IPv6, and why aren't we there yet? https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html (Haettu 15.12.2019).

TechTerms. 2015. IEE. https://techterms.com/definition/ieee (Haettu 23.2.2020).

Vasudeva, Amol ja Sood, Manu. 2018. Survey on Subil Attack Defense Mechanisms in Wireless Ad Hoc Networks. *Journal of Network and Computer Applications* 120 (2018): 78–118.

Walls, Colin. 2012. *Embedded Software the Works*.2nd ed. Amsterdam: Newnes, 2012. Chapter 8: 304-304.

Wedd, Michael. 2018. What is LPWAN and the LoRaWAN Open Standard? https://www.iotforall.com/what-is-lpwan-lorawan/ (Haettu 23.12.2019).

Wilton, Thomas. 2019. How to Solve a Destination Host Unreachable Error. https://www.lifewire.com/how-to-solve-destination-host-unreachable-error-4686734 (Haettu 23.2.2020).

Zheng, Jianliang ja Lee, Myung. 2004. A comprehensive performance study of IEEE 802.15.4. IEEE Press.