jamk

Kyberturvallisuus haavoittuvuudet IoT-ympäristössä – Case eÄlytelli

Paulus Pursiainen

Opinnäytetyö
Toukokuu 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Pursiainen Paulus

Kyberturvallisuus haavoittuvuudet IoT-ympäristössä – Case eÄlytelli

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2022, 41 sivua.

Tietojenkäsittely ja tietoliikenne. Tieto ja viestintätekniikka. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Opinnäytetyön tavoitteena oli tutkia yleisesti IoT-järjestelmiin kohdistuvia haavoittuvuuksia, sekä mitkä niistä ovat eÄlytelli-hankkeen JAMK:in pilotteihin kohdistuvia haavoittuvuuksia.

Opinnäytetyössä selvitettiin minkälainen IoT:n rooli voisi olla tulevaisuudessa, sekä minkälaisia uhkia siihen kohdistuu. IoT:hen liittyviä haavoittuvuuksia ja uhkia tutkittiin viidessä eri kerroksessa. Havaintokerroksella tutkittiin laitteita ja antureita. Verkkokerroksella tutkittiin tietoliikenneratkaisuja. Käsittelykerroksella tutkittiin dataa käsitteleviä väliohjelmia. Sovelluskerroksella tutkittiin sovelluksia ja pilvialustaa. Yrityskerroksella tutkittiin järjestelmään liittyvän organisaation sääntöjä ja käytäntöjä. Näiltä kerroksilta löytyneitä haavoittuvuuksia tutkittiin myös kahdesta eÄlytelli-hankkeen pilotista. Tutkimus perustui kirjallisuuteen.

Piloteista löytyi useita haavoittuvuuksia eri kerroksilta, osa haavoittuvuuksista liittyi useaan kerrokseen. Kummassakin pilotissa oli lähes samat haavoittuvuudet. Pilottien kyberturvallisuuden tutkiminen voisi jatkua haavoittuvuuksien hyväksikäytön todennäköisyyden arvioinnilla, sekä haavoittuvuuksien testaamisella.

Avainsanat (asiasanat)

esineiden internet, kyberturvallisuus

jamk

Description

Pursiainen Paulus

Kyberturvallisuus haavoittuvuudet IoT-ympäristössä – Case eÄlytelli

Jyväskylä: JAMK University of Applied Sciences, May 2022, 41 pages.

Engineering and Technology. Degree Programme in information- and Communication Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

The purpose of the thesis was to investigate the vulnerabilities of IoT systems in general, as well as the vulnerabilities of the eÄlytelli-project pilots.
Thesis studied the role of IoT in the future, as well as what kind of threats it could have. Vulnerabilities and threats of IoT were investigated at five different layers. Devices and sensors were examined in the perception layer. At the network layer, telecommunication solutions were studied. The processing layer was used to examine the data processing middleware. At the application layer, applications and the cloud platform were studied. In the business layer the rules and practices of the organization involved in the system was studied. Vulnerabilities found in these layers were also investigated in two eÄlytelli-project pilots. The study was based on literature.
Several vulnerabilities were found in the pilots from different layers, some of the vulnerabilities were related to multiple layers. Both pilots had almost the same vulnerabilities. Research about the cyber security of pilots could continue by assessing the likelihood of exploiting the vulnerabilities, as well as testing the vulnerabilities.

Keywords/tags

Internet of things, Cybersecurity

Sisältö

1 Johdanto 6
2 Mikä IoT? 7
2.1 Toimintaketju 8
2.2 Tietoliikenneratkaisut 10
2.3 IoT:n tulevaisuus 12
2.4 Kyberhyökkäysten yleistyminen 14
3 IoT-kerrokset ja niihin liittyvät uhat 17
3.1 Havaintokerros 19
3.2 Verkkokerros 21
3.3 Käsittelykerros 22
3.4 Sovelluskerros 22
3.5 Yrityskerros 24
3.6 Riskienhallinta 24
3.7 OWASP TOP 10 26
4 Tutkimuksen kohteet 28
4.1 Pilotti Sammakkokangas 28
4.2 Pilotti VAPO 30
5 Tulokset 31
5.1 Havaintokerros 31
5.2 Verkkokerros 32
5.3 Käsittelykerros 33
5.4 Sovelluskerros 33
5.5 Yrityskerros 34
5.6 Yhteenveto 34
6 Johtopäätökset ja pohdinta 36
Lähteet 38

Kuviot

Kuvio 1 IoT voidaan jakaa kolmeen eri luokkaan (Yritysjohdon opas IoT:n ja teollisen internetin hyödyntämiseen n.d.). 7
Kuvio 2 Esimerkki toimintaketjusta. 9
Kuvio 3 Yhdyskäytävän toiminta (Kelly 2020). 10
Kuvio 4 Yhteyden nopeuden ja virrankulutuksen suhde kantamaan (Hertog 2019). 11
Kuvio 5 Verkkoon yhdistettyjen laitteiden määrä (Cisco Annual Internet Report 2020). 13
Kuvio 6 Kyberhyökkäyksien määrän kasvu (Bissel, Fox, LaSalle & Cin 2021, 8). 15
Kuvio 7 Kyberhyökkäyksien kustannukset yrityksille (Bissel, Lasalle & Dal Cin 2019, 20)..... 16
Kuvio 8 Hyökkäysten määrät eri aloilla (Ray, Marshall, Boyce, De Sousa & Foster 2021, 6). 16
Kuvio 9 IoT:n jako viiteen kerrokseen. 19
Kuvio 10 Man-in-the-Middle hyökkäys(Man in the Middle (MITM) Attack n.d.). 22
Kuvio 11 Esimerkki uhkapuusta 25
Kuvio 12 Tärkeimmät haavoittuvuudet (Basatwar 2021). 26
Kuvio 13 Järjestelmän kuvaus (kuva Heli Sutinen). 29

Taulukot

Taulukko 1 Piloteista löytyneiden haavoittuvuuksien määrä. 35

1 Johdanto

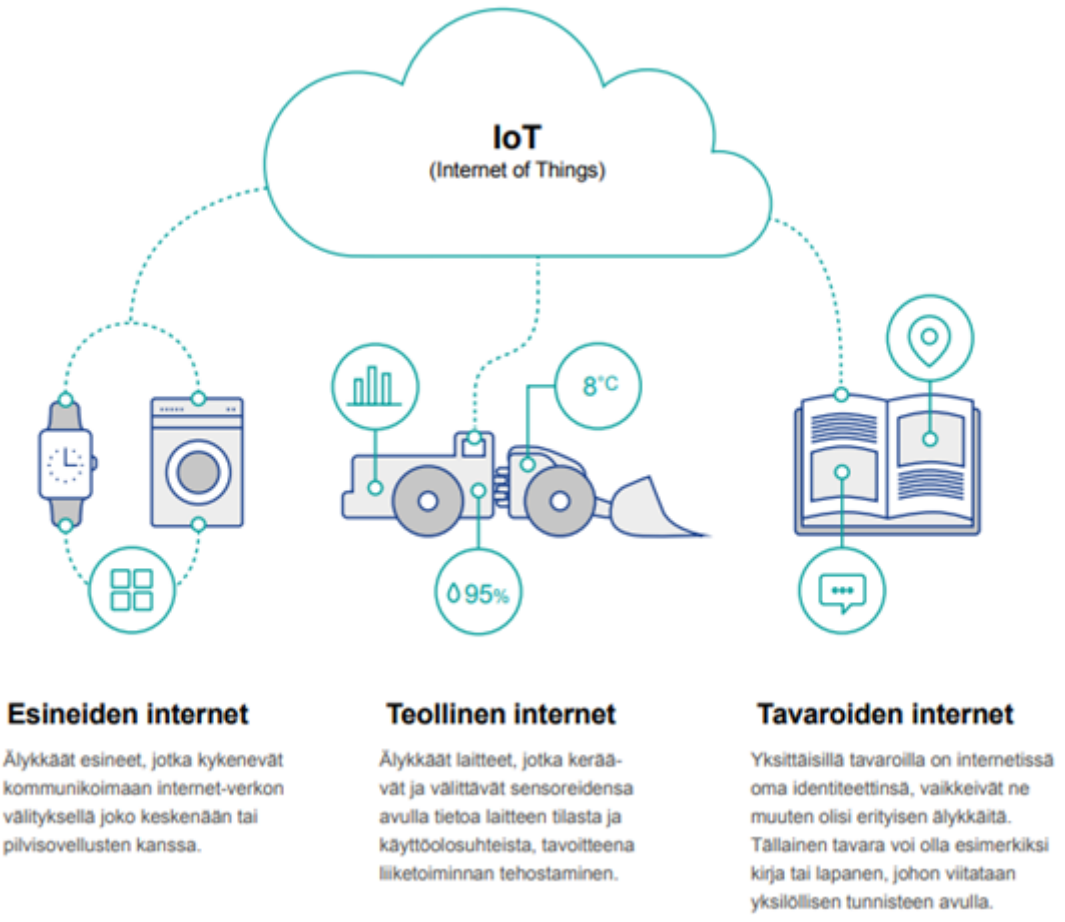
Turvallisuus on yksi isoimmista IoT-teknologiaa koskevista huolenaiheista. IoT:n suosion kasvaessa yritysten ja kotitalouksien käytössä, kyberhyökkäyksien pelätään tulevaisuudessa yleistyvän. Tärkeimpiä asioita uusien IoT-ratkaisujen suunnittelussa onkin turvallisuus. (Bissel, Fox, LaSalle & Cin 2021, 8; Chaudhuri 2019.)

Tämän opinnäytetyön tarkoituksena on tutkia kahden eÄlytelli-hankkeessa kehitetyn IoT-ratkaisun kyberturvallisuutta. Tutkimuksen kohteena ovat Sammakkokangas Oy:n kanssa kehitetty järjestelmä, jonka tarkoituksena on tunnistaa ja ennakoida sekajätteen itsesyttymistä, sekä Vapo Oy:n kanssa kehitetty turpeen keräyksen reaaliaikainen seurantajärjestelmä. Opinnäytetyön tavoitteena on tutkia yleisesti IoT-järjestelmiin kohdistuvia haavoittuvuuksia, sekä mitkä niistä ovat eÄlytelli-hankkeen JAMK:in pilotteihin kohdistuvia haavoittuvuuksia. Opinnäytetyö perustuu kirjallisuustutkimukseen. Tässä kirjallisuustutkimuksessa tarkastellaan IoT-järjestelmien kyberturvallisuutta kokoamalla ja analysoimalla IoT:n kyberturvallisuuteen liittyvää tutkimusaineistoa. Tarkoituksena on tutkimusaineiston perusteella määrittää mahdollisimman tarkasti ja kattavasti pilotteihin liittyvät haavoittuvuudet ja vertailla niitä keskenään. Luotettaviin tuloksiin pyritään käyttämällä laajaa tutkimusaineistoa, sekä haavoittuvuuksien tarkalla kuvaamisella.

Opinnäytetyön toimeksiantajana toimii eÄlytelli-hanke (ekologiset, älykkäät ja turvalliset teollisen internetin palvelut). eÄlytelli on Jyväskylän Yliopiston ja Jyväskylän ammattikorkeakoulun IT-instituutin yhteistyöhanke. Hankkeessa on mukana eri toimialojen yhteistyökumppaneina toimivia yrityksiä. Hankkeessa kehitetään osaamista ja ratkaisuja, joilla yhteistyökumppaneiden kanssa pilotoidaan ekologisia, älykkäitä ja turvallisia internetin palveluita. Hankkeen rahoittajina toimii Euroopan aluekehitysrahasto (EAKR). Hanke alkoi toukokuussa 2019 ja päättyi joulukuun 2021 lopussa. (eÄlytelli-hanke, 2021.)

2 Mikä IoT?

Esineiden internet, englanniksi Internet of Things (IoT) on laaja käsite ja sen määritelmä varsinkin suomen kielessä on häilyvä. Yhden määritelmän mukaan IoT koostuu laitteista, jotka pystyvät lähettämään toisilleen dataa verkon yli ilman ihmisen apua. IoT:ksi voidaan siis lukea melkein kaikki verkkoon yhdistetyt laitteet älypolttimosta autoon tai kodin turvajärjestelmään. (Gilchrist 2017, 5.) Laaja IoT käsite voidaan jakaa myös kolmeen pienenpään luokkaan: esineiden internet, teollinen internet ja tavaroiden internet (ks. kuvio 1). Näitä termejä käytetään usein myös rinnakkain ja niiden merkitykset vaihtelevat. (Yritysjohdon opas IoT:n ja teollisen internetin hyödyntämiseen n.d.)



Kuvio 1 IoT voidaan jakaa kolmeen eri luokkaan (Yritysjohdon opas IoT:n ja teollisen internetin hyödyntämiseen n.d.).

Teollisuudessa käytettäviä yleensä monimutkaisempia ratkaisuja kutsutaan teolliseksi internetiksi, englanniksi Industrial Internet of Things (IIoT). Älykkäillä IoT-ratkaisuilla voidaan auttaa yrityksiä tekemään niiden toiminnasta varmempaa ja tehostamaan niiden liiketoimintaa. Teollisen internetin ratkaisuissa saatetaan käyttää apuna koneoppimista. (Marr 2018.)

Suuret järjestelmät keräävät ja käyttävät erittäin paljon dataa. Kun tätä monimuotoista dataa analysoidaan ja käytetään, puhutaan monesti Big Datasta. Big Data on vahvasti yhteydessä IoT:hen. IoT luo ja tarvitsee Big Dataa, Big Data vaatii hyvää analytiikkaa ja hyvä analytiikka vastaavasti kehittää IoT-järjestelmiä ja niiden prosesseja. (Kundhavai & Sridevi 2016, 10-11.)

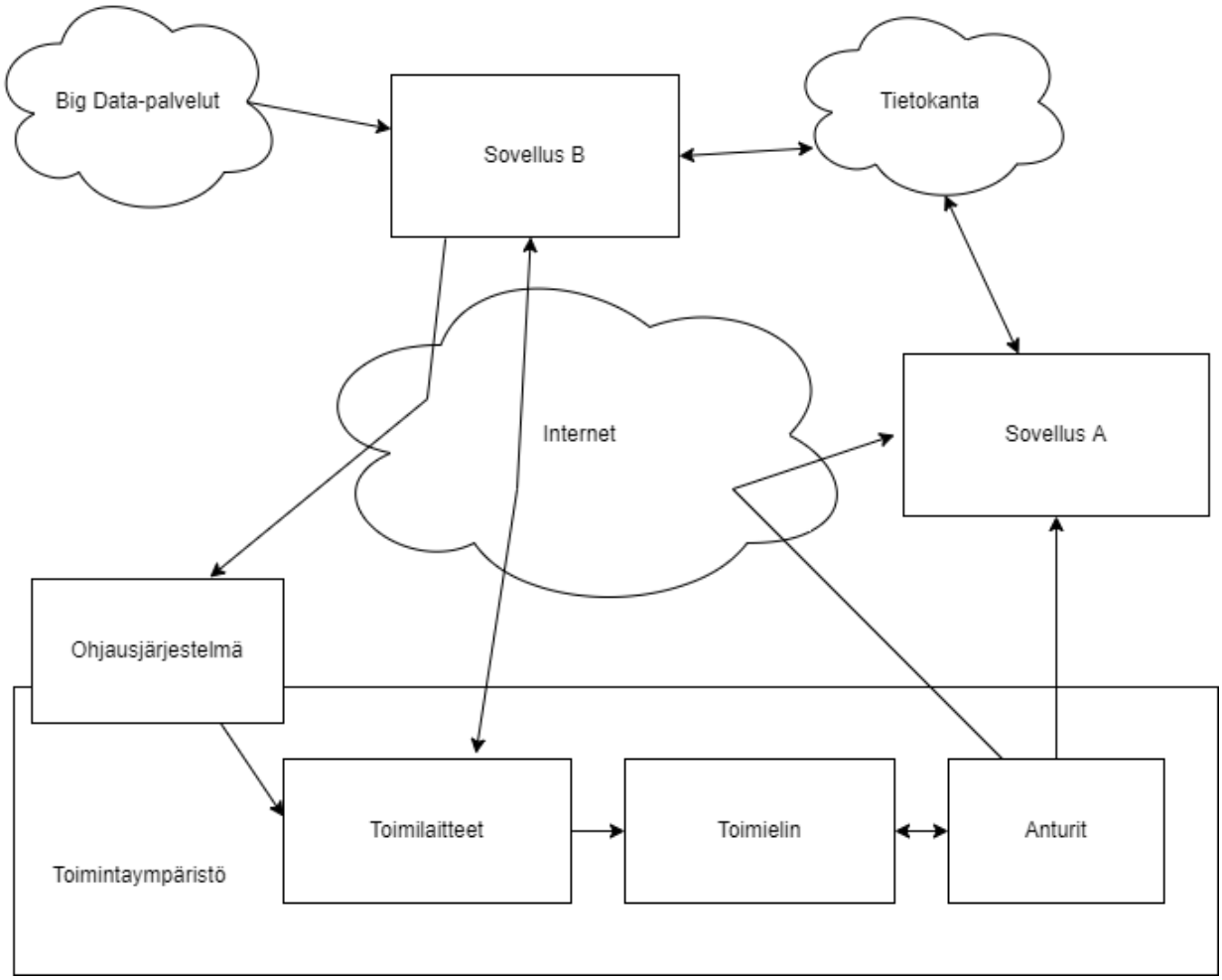
IIoT ei välttämättä tarvitse pilvipalveluita toimiakseen, mutta teollisuuden käyttämissä ratkaisuissa pilvipalvelut mahdollistavat suurien data määrien keräämisen ja tutkimisen tehokkaasti. Jokaiseen ratkaisuun pelkästään pilvessä tehtävä datan prosessointi ei riitä esimerkiksi liian suuren viiveen takia, tällöin voidaan käyttää reunalaskentaa. Reunalaskennassa dataa käsitellään mahdollisimman lähellä datan keräyspaikkaa viiveen pienentämiseksi, sekä varmuuden parantamiseksi. (Chang & Wu 2021, 35.) Teollisuudessa käytetyt ratkaisut mullistavat tapaa tuottaa tavaroita. Muutos niin suuri, että usein puhutaan Industry 4.0:sta, eli neljännestä teollisesta vallankumouksesta. (Marr 2018.)

Tavaroiden internetissä olevat laitteet eivät välttämättä ole erityisen älykkäitä, mutta ne kuitenkin kommunikoivat internetin yli toisille laitteille. Esineiden internetillä, kuten muillakin IoT-laitteilla, on lukematon määrä käyttötarkoituksia. Esimerkiksi olkoon kirjaan lisätty tunniste, jonka avulla sitä seurataan kirjastossa. (Yritysjohdon opas IoT:n ja teollisen internetin hyödyntämiseen n.d.)

2.1 Toimintaketju

IoT-järjestelmän toimintaa voidaan havainnollistaa toimintaketjun avulla (ks. kuvio 2). Tähän esimerkki IoT-ympäristöön kuuluvat: ohjausjärjestelmä, toimilaitteet, toimielin, anturit, sovellus a ja b, tietokanta ja Big Data palvelut. Toimintaketjun tarkastelu voidaan aloittaa esimerkiksi antureista. Anturit ovat elektronisia laitteita, jotka tuottavat dataa fyysisestä tilasta tai tapahtumasta.

Anturit voivat yksinkertaisimmillaan vain kerätä dataa, jota tutkitaan ja käsitellään muualla. Anturit lähettävät datan verkon yli sovellus A:lle. Anturit ovat yhteydessä yhdyskäytävään, jossa dataa voidaan jo käsitellä ennen sen lähettämistä sovellukselle internetin yli. (Hautamäki 2021.)



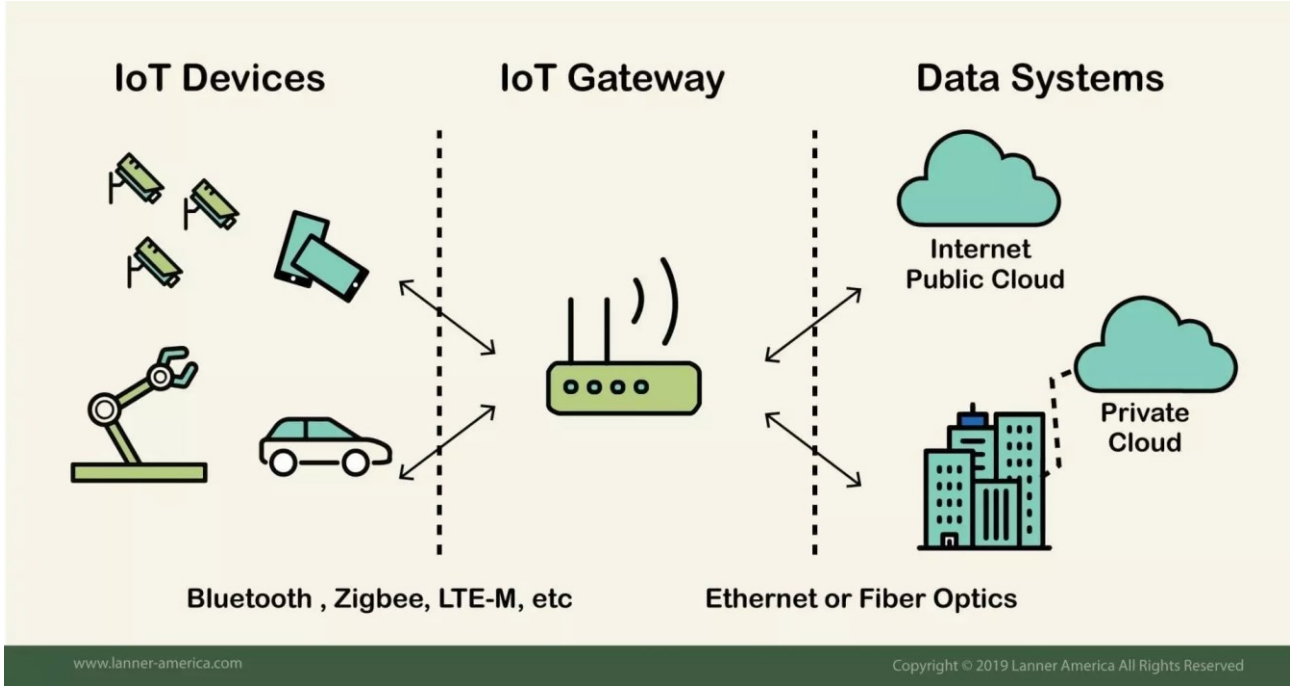
Kuvio 2 Esimerkki toimintaketjusta.

Sovellus A vastaanottaa datan ja tallentaa sen tietokantaan sopivassa muodossa. Sovellus B lukee dataa tietokannasta, sekä voi yhdistää sitä hakemaansa Big Dataan. Sovellus muuttaa datan käytettäväksi informaatioksi ja välittää sen ohjausjärjestelmälle tai suoraan toimilaitteille. Ohjausjärjestelmä muuttaa toimilaitteiden toimintaa saamansa informaation avulla. Sovellus B sisältää myös käyttöliittymän, josta voidaan säätää laitteen toimintaa kerätyn datan mukaan. Sovellus voi

myös esimerkiksi mahdollistaa ohjausjärjestelmän tai toimilaitteiden käsikäytön tai lähettää hälytyksen käyttäjälle poikkeustilanteista. (Hautamäki 2021.)

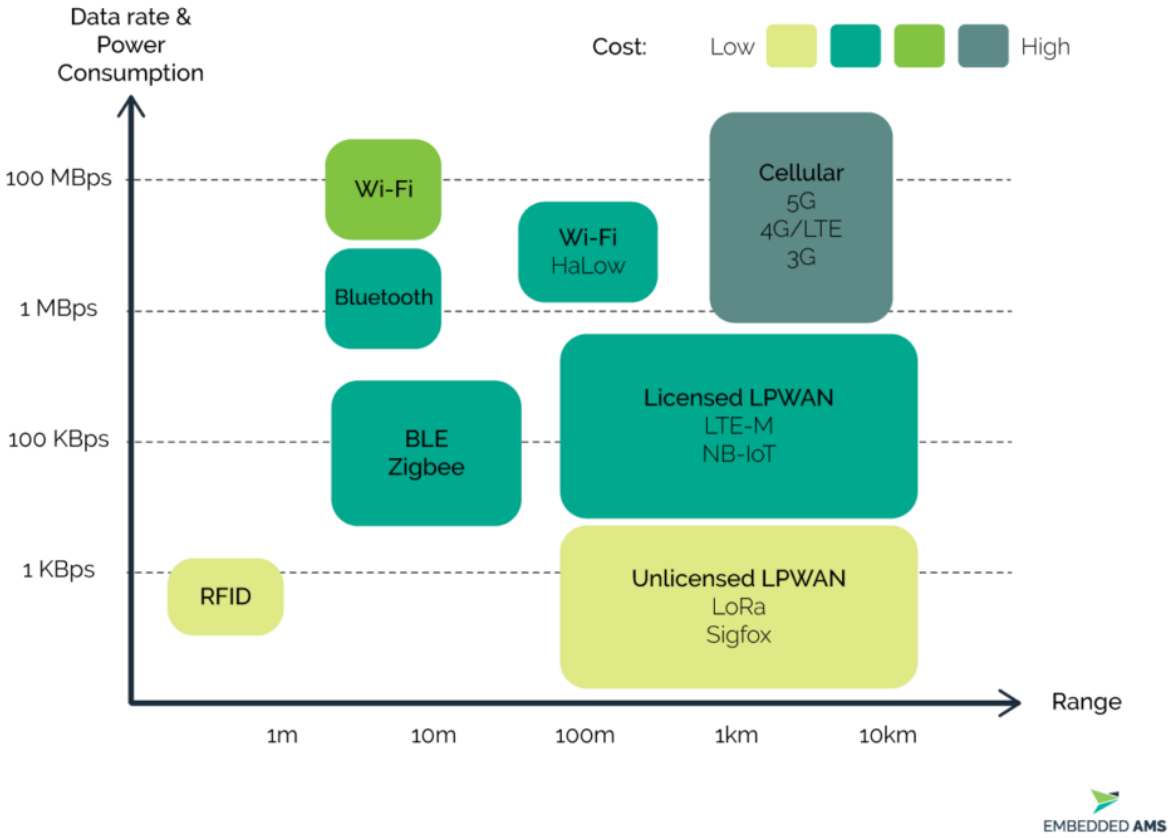
2.2 Tietoliikenneratkaisut

Monimutkaisissa ratkaisuissa tietoa voidaan kerätä useilla erilaisilla antureilla. Jotta eri yhteyksiä käyttävät IoT-laitteet ja pilvessä olevat sovellukset ja tietokanta saadaan kommunikoimaan keskenään, tarvitaan yhdyskäytävä. Yhdyskäytävä mahdollistaa pelkän tietoliikenne yhteyden lisäksi myös jonkin tasoista reunalaskentaa. Yhdyskäytävä pystyy esimerkiksi suodattamaan useiden antureiden suuresta datamäärästä vain sovellukselle tarpeellisen tiedon ja näin mahdollistamaan varmemman yhteyden laitteiden ja sovellusten välillä. Yhdyskäytävä mahdollistaa myös turvallisemman suojatun yhteyden internetin yli. Sillä voidaan yhdistää useampi eri datansiirtotapa saman suojatun yhteyden alle. Suojaamaton yhteys laitteen ja sovelluksen välillä olisi suuri tietoturvariski koko IoT-järjestelmälle. Yhdyskäytävä mahdollistaa myös laitteiden pitkän akun keston, sillä reitittimen sijoittelulla voidaan vähentää laitteen lähettimen tehoa. (Kelly 2020.)



Kuvio 3 Yhdyskäytävän toiminta (Kelly 2020).

IoT-laitteet vaativat tietoliikenneyhteyden lähettääkseen kerättyä dataa sitä käsittelevälle sovellukselle, sekä saadakseen mahdollisen vastauksen sovellukselta. IoT-ratkaisujen laajan kirjon vuoksi, myös tietoliikenteessä käytettäviä tekniikoita on lukuisia. Uutta IoT-ratkaisua suunniteltaessa, yhteyden valinnassa kolme suurinta tekijää ovat lähetettävän ja vastaanotettavan datan määrä, kantama, virrankulutus, sekä hinta (ks. kuvio 3). Jokaisella yhteydellä on omanlaiset ominaisuutensa. (Hertog 2019.)



Kuvio 4 Yhteyden nopeuden ja virrankulutuksen suhde kantamaan (Hertog 2019).

Wi-Fi on laajasti julkisissa paikoissa ja kotitalouksissa käytetty langaton verkko. Wi-Fi on erittäin tehokas ja helposti IoT-ratkaisujen käyttöön muokattava ratkaisu. Verkon ylläpito on hieman kalliimpaa verrattuna joihinkin muihin tiedonsiirto teknologioihin, mutta jos paikalla on jo valmiiksi

rakennettu ja ylläpidetty Wi-Fi-verkko, voidaan hinta laskea hieman pienemmäksi. Monet kotitalouksiin tarkoitetuista IoT-laitteista käyttävätkin Wi-Fi:ä, koska lähes joka kodissa on jo valmiiksi olemassa oleva Wi-Fi-verkko. Wi-Fi:n laaja kattavuus tekee IoT-laitteiden liikuttamisesta helppoa ja uuden laitteen saa liitettyä verkkoon hyvin vaivattomasti. Muita hyviä puolia Wi-Fi-verkossa on sen hyvä tiedonsiirtokyky, sekä sisätiloihin sopiva kantama. Heikkoutena Wi-Fi:ssä on suuri virrankulutus, minkä vuoksi se ei sovi akulla tai paristoilla toimiviin ratkaisuihin. Myös lyhyt kantama rajoittaa Wi-Fi:n käyttöä esimerkiksi ulkona. (Hertog 2019).

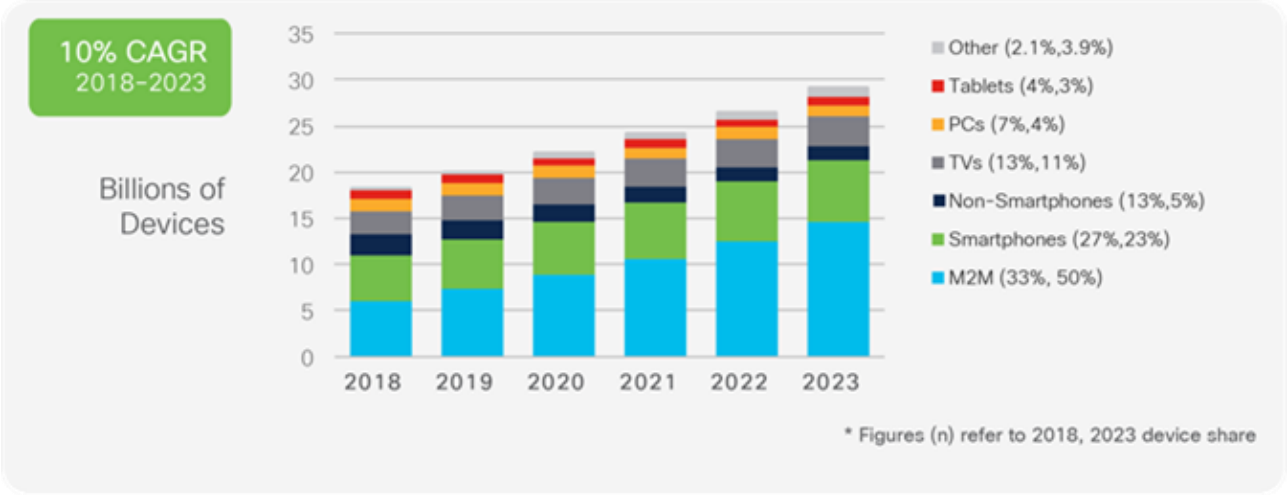
LORA on Semtech:in omistama, LPWAN kategoriaan kuuluva modulaatioratkaisu. LORAWAN on siihen perustuva verkkoprotokolla. LORAWAN on avoin kommunikointi standardi, jonka kehitystä hallinnoi voittoa tavoittelematon LoRa Alliance-järjestö. Järjestöön kuuluvat esimerkiksi Cisco, IBM ja Suomessa LORAWAN yhteyksiä tarjoava Digita. LORAWAN on langaton teknologia, jonka kantama on normaalisti noin 15 kilometriä ja parhaissa olosuhteissa jopa kolme kertaa pidempi. Maaston profiili voi vaikuttaa kantavuuteen huomattavasti. LORAWAN on vähätehoinen ja tarkoitettu pienten datamäärien lähettämiseen ja vastaanottamiseen. Yleensä datamäärät ovat muutamia kymmeniä tavuja. Vähätehoisuuden ansiosta laitteiden akun kesto on erittäin hyvä. Yksinkertaisen anturin virtalähteenä voidaan käyttää 9 voltin paristoa ja sen kesto voi olla jopa 10 vuotta. Tavallisesti datan lähetystiheys on 15–60 minuuttia. (Kuukka n.d.)

Mobiilidatayhteys on myös pitkän kantaman omaava teknologia. Neljännen sukupolven eli 4G-tekniikan avulla datan enimmäisnopeus on noin 1Gbit/s ja uusimman sukupolven 5G-tekniikka voi mahdollistaa jopa 10Gbit/s siirto nopeudet. Mobiilidatayhteys on suosittu tapa yhteyden rakentamiseen IoT-ratkaisuissa, sen huonona puolena on korkea hinta, sekä virran kulutus. (Hertog 2019; Segarra 2022.) Muita IoT-ratkaisuissa käytettyjä yhteyksiä ovat esimerkiksi Bluetooth, BLE, Zigbee ja RFID (Hertog 2019; Sethi, P. & Sarangi, S. 2017).

2.3 IoT:n tulevaisuus

IoT- laitteiden, sekä -ratkaisujen määrä on kasvanut viime vuosina räjähdysmäisesti. Kasvu näkyy hyvin muun muassa IoT-järjestelmissä käytetyissä M2M-yhteyksien (koneiden välisien yhteyksien)

määrässä, joidenka uskotaan tulevaisuudessa kattavan yli puolet kaikista eri laitteiden käyttämistä yhteyksistä (ks kuvio 5). Aikaisemmin yhteyksien määrässä älypuhelinten yhteydet olivat samalla tasolla M2M-yhteyksien kanssa. Ciscon arvion mukaan vuonna 2023 internettiin yhdistettyä laitetta tulee olemaan 3.6 jokaista maailman ihmistä kohden. (Cisco Annual Internet Report 2020.) IoT-markkinoiden arvon uskotaan nousevan jopa 1386 miljardiin dollariin vuoteen 2026 mennessä, kun se vuonna 2020 oli noin 761 miljardia dollaria (Crane 2021). Covid-19 viruksella ei näyttäisi olevan hidastavia vaikutuksia IoT:n kehittymiselle. Microsoftin kyselyn mukaan vuonna 2020 noin kolmannes organisaatiosta oli valmiita sijoittamaan lisää IoT-ratkaisuihin. Vastaavasti vuonna 2021 organisaatiosta jo lähes puolet olivat valmiita siihen. (IoT Signals 2021.)



Kuvio 5 Verkkoon yhdistettyjen laitteiden määrä (Cisco Annual Internet Report 2020).

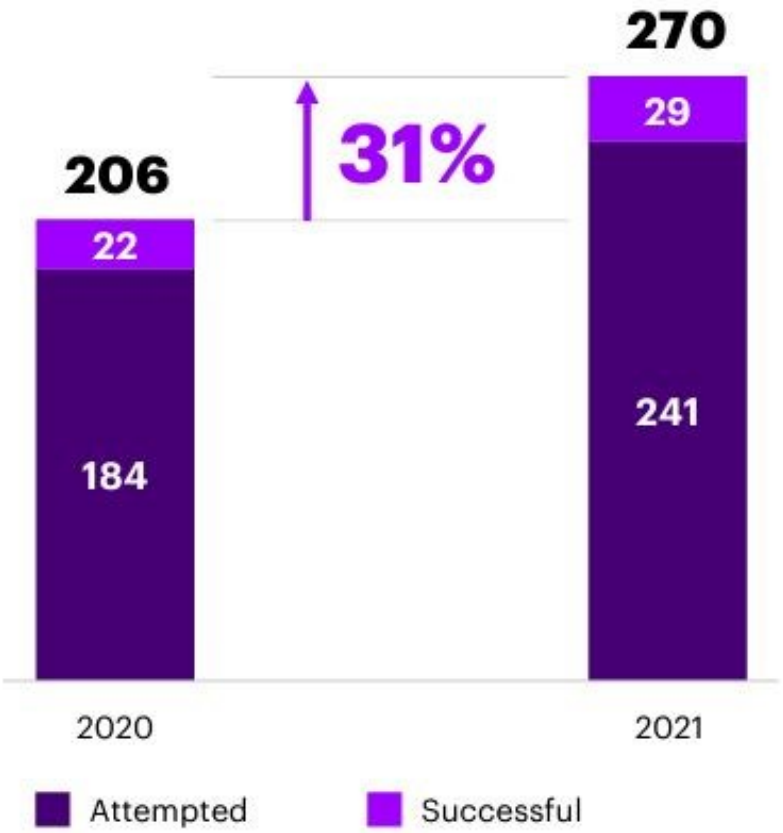
Turvallisuushaasteet voivat hidastaa IoT:n kasvua. Nopeasti yleistyneet IoT-ratkaisut voivat kohdata tulevaisuudessa turvallisuusrajoituksia ja -haasteita. Suuri osa yritysten ratkaisuista ovat turvallisuuden osalta puutteellisia. Kun suuria määriä dataa säilytetään ja siirretään verkossa, mahdollisuus tietovuotoon on suuri. Useat teollisuuden toimijat ovat joutuneet hyökkäyksien kohteeksi, joissa koitetaan päästä käsiksi yrityksen yksityiseen dataan. Internettiin yhdistettyjen laitteiden määrän kasvaessa myös huoli turvallisuudesta kasvaa, joka taas voi vaikuttaa IoT:n

yleistymiseen negatiivisesti. Kysyntä uusille älykkäille ratkaisuille näyttäisi kuitenkin pysyvän suurena ja jopa edellä tarjontaa. (Chaudhuri 2019.)

Teknologian sekä internetyhteyksien kehitys avaa uusia mahdollisuuksia IoT:n soveltamiselle. Tutkimus uuden sukupolven langattoman datayhteyden parissa on vasta alussa, mutta tulevaisuudessa 6G yhteyksien odotetaan pystyvän siirtämään valtavia määriä dataa lähes viiveettömästi. Kun lähes kaikki laitteet ja koneet ovat yhteydessä internettiin, voidaan puhua kaiken internetistä, englanniksi Internet of Everything (IoE). IoE voi tulla mahdollistamaan älykaupungit tai todellisuudesta erottumattoman laajennetun todellisuuden (XR). (Padhi & Charrua-Santos 2021, 13.)

2.4 Kyberhyökkäysten yleistyminen

Kyberhyökkäysten määrä jatkaa kasvuaan. Accenturen mukaan vuonna 2021 jokaista yritystä kohtaan tehtiin keskimäärin 270 hyökkäystä. Tutkimuksessa hyökkäyksiksi luettiin luvattomat yritykset päästä käsiksi yrityksien dataan, sovelluksiin, palveluihin, verkkoihin tai laitteisiin. Hyökkäysten määrä kasvoi 31% verrattuna vuoteen 2020, kuten on havainnollistettu kuviossa 6. Kyberhyökkäysten yleistyessä, myös yritysten panostus kyberturvallisuuteen kasvaa kovaa vauhtia. (Bissel, Fox, LaSalle & Cin 2021, 8-9.) Accenturen mukaan vuonna 2021 merkittäviä tapauksia olivat useat kohteen sidosryhmän tai kolmannen osapuolen sovelluksien tai laitteiden haavoittuvuuden kautta tehdyt hyökkäykset. Myös backdoor-haavoittuvuuksia löytyi paljon. Backdoor-haavoittuvuuksissa järjestelmään jätetään huomaamaton haavoittuvuus, jota voidaan myöhemmin käyttää hyväksi. (Ray, Marshall, Boyce, De Sousa & Foster 2021, 10.)



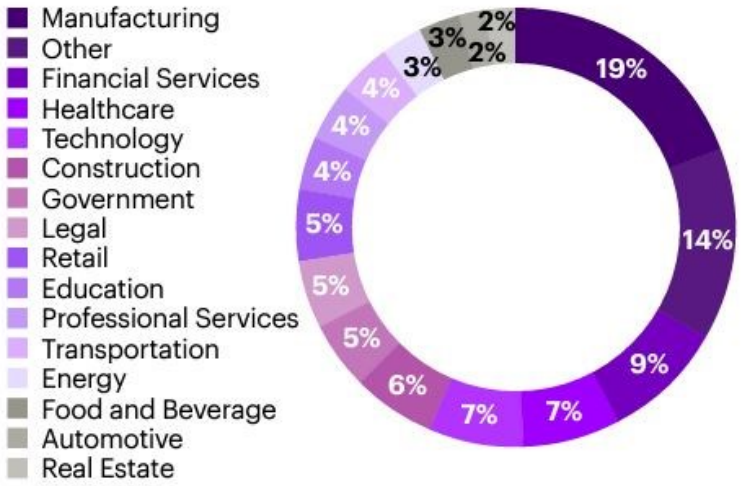
Kuvio 6 Kyberhyökkäyksien määrän kasvu (Bissel, Fox, LaSalle & Cin 2021, 8).

Samalla kun hyökkäysten määrä kasvaa, kasvaa myös niiden vaikutus yrityksiin. Kyberhyökkäysten aiheuttamat kustannukset kostuvat esimerkiksi tiedon menetyksestä ja sen aiheuttamasta häiriöstä yritystoimintaan. Isoimmat vahingot yrityksille aiheuttavat haittaohjelmat, verkkopohjaiset hyökkäykset, sekä palvelunestohyökkäykset. Kuvio 7 esittää, kuinka eri hyökkäykset vaikuttavat kustannuksiin, sekä mistä kustannukset koostuvat. Kuviossa oranssi väri esittää jokaisen hyökkäystyypin suurinta kustannusosuutta. Esimerkiksi haittaohjelmat aiheuttavat eniten rahallista vahinkoa tiedon menetyksen kautta, mutta niiden vaikutus näkyy myös liiketoiminnan häiriöinä, tulojenmenetyksenä, sekä laitteiden hajoamisena. (Bissel, Lasalle & Dal Cin 2019, 18-21.)

	Business disruption	Information loss	Revenue loss	Equipment damage	Total cost by attack type
Malware (+11%)	$ 0.5	$ 1.4	$ 0.6	$ 0.1	$ 2.6
Web-based attacks (+17%)	$ 0.3	$ 1.4	$ 0.6	$ –	$ 2.3
Denial-of-service (+10%)	$ 1.1	$ 0.2	$ 0.4	$ 0.1	$ 1.7
Malicious insiders (+15%)	$ 0.6	$ 0.6	$ 0.3	$ 0.1	$ 1.6
Phishing and social engineering (+8%)	$ 0.4	$ 0.7	$ 0.3	$ –	$ 1.4
Malicious code (+9%)	$ 0.2	$ 0.9	$ 0.2	$ –	$ 1.4
Stolen devices (+12%)	$ 0.4	$ 0.4	$ 0.1	$ 0.1	$ 1.0
Ransomware (+21%)	$ 0.2	$ 0.3	$ 0.1	$ 0.1	$ 0.7
Botnets (+12%)	$ 0.1	$ 0.2	$ 0.1	$ –	$ 0.4
Total cost by consequence	$ 4.0	$ 5.9	$ 2.6	$ 0.5	**$ 13.0**

Kuvio 7 Kyberhyökkäyksien kustannukset yrityksille (Bissel, Lasalle & Dal Cin 2019, 20).

Lunnaita vaativat kiristysohjelmat ovat lisääntyneet ja ne kattavat lähes 35% kaikista vuonna 2021 tehdyistä hyökkäyksistä. Eniten kiristysohjelmat piinaavat valmistus, rahoituspalvelu, terveydenhuolto ja teknologia-aloja. Hyökkäysten määrää eri aloja kohtaan kuvaa kuvio 8. (Ray, Marshall, Boyce, De Sousa & Foster 2021, 6.)



Kuvio 8 Hyökkäysten määrät eri aloilla (Ray, Marshall, Boyce, De Sousa & Foster 2021, 6).

Suomessa käytävä Nato-keskustelu voi suojelupoliisin mukaan näkyä Venäjän vaikuttamisyrityksinä. Toistaiseksi Venäjä näyttää sitovan resurssinsa Ukrainaan, mutta tilanne voi muuttua nopeasti. Venäjän yksi tapa vaikuttaa on kyberhyökkäykset. Suurin osa näistä hyökkäyksistä koostuu palvelunestohyökkäyksistä, sekä verkkosivujen töhrinnästä. Näillä koitetaan luoda mielikuvaa yhteiskunnan lamaantumisesta, vaikka ne eivät todellisuudessa olisi vaaraksi yhteiskunnan toiminnalle. Suojelupoliisi kuitenkin kertoo, että vakavampienkin hyökkäysten uhka on kohonnut ja esimerkiksi energianjakelun ja muun kriittisen infrastruktuurin ohjauselektroniikan suojaamiseen on nyt panostettava. (Supon vuosikirja 2021: Suomalaisten on varauduttava Venäjän vaikuttamisyrityksiin Nato-keskustelun aikana 2022.)

3 IoT-kerrokset ja niihin liittyvät uhat

IoT-ratkaisut eivät ole täysin turvallisia. Kun ratkaisut keräävät tietoa käyttäjästä, laitteesta tai laitteen ympäristöstä, tietoturva on erityisen tärkeää ja yksityisyyden suoja on otettava huomioon. (Chaudhuri 2019.) Tietoturvalla pyritään ylläpitämään järjestelmässä kolmea tärkeää asiaa: saatavuutta, eheyttä ja luottamuksellisuutta. Saatavuudella tarkoitetaan, että järjestelmän käyttäjien täytyy päästä käyttämään sitä. Eheys tarkoittaa, että järjestelmää tai sen sisältämää tietoa pystyy muokkaamaan vain sen käyttäjät. Luottamuksellisuutta, järjestelmän tietoja voi käsitellä vain sen käyttäjät. Haavoittuvuus on heikkous järjestelmässä, joka mahdollistaa hyökkäyksen tai järjestelmän vahingoittamisen. Haavoittuvuus voi olla esimerkiksi järjestelmän käyttötavassa, sen suunnittelussa tai sen toteutuksessa. Haavoittuvuutta hyväksikäyttäen voidaan toteuttaa suojattavaan kohteeseen liittyvä uhka. Uhkia pyritään torjumaan hallitsemalla haavoittuvuuksia. (Pfleeger & Pfleeger 2012, 8-19.)

IoT-ratkaisut voivat olla hyvin monimutkaisia ja keskenään erilaisia. Tämä tekee yhtenäisten turvallisuustekniikoiden käytöstä vähintäänkin haastavaa. IoT-laitteiden turvallisuutta normaaliin tietokoneeseen tai verkkoon verrattuna vaikeuttavat heikkotehoinen tiedonsiirto, riittävän tehokkaiden salausalgoritmien puute laitteiden vähäisen laskentakyvyn vuoksi, laitteiden suuri määrä isolla alueella monimutkaisten järjestelmien luomiseksi, sekä laitteiden päivitettävyys. Useiden laitteiden kokonaisuuksissa valmistajan ohjelmistopäivitysten loppuessa, laitteiden vaihto voi tulla

kalliiksi. IoT-laitteesta löytyvää tietoturva-aukkoa voi olla mahdollista käyttää jopa tuhansia samanlaisia laitteita vastaan. (Chaudhuri 2019.)

Kuten muihinkin tietojärjestelmiin tai -verkkoihin, IoT-ratkaisuihin kohdistuneiden hyökkäyksien takana oleva tekijät ja heidän motivaationsa vaihtelevat. Yksittäinen hyökkääjä voi haluta vain näyttää kykynsä murtaa esimerkiksi jonkin kaupallisen IoT-tuotteen turvallisuus. Hyökkääjänä voi toimia myös valtio, jolloin motivaationa voi olla salaisen tiedon kerääminen tai pelkän tuhon aiheuttaminen. Poliittisen ryhmät voivat hyökätä heidän mielestänsä korruptoituneita organisaatioita vastaan tarkoituksenaan aiheuttaa tuhoa ja tuoda julki organisaation toimintaa. Motivaationa voi toimia myös taloudellinen hyöty. Rikolliset voivat esimerkiksi kaapata laitteita tai tietoa ja vaatia lunnaita näitä vastaan. Useiden laitteiden kokonaisuuksilla voi olla myös mahdollista louhia kryptovaluuttaa tai käyttää niitä palvelunestohyökkäyksien toteuttamiseen, joita myydään palveluna eteenpäin. (IoT Attacks, Hacker Motivations, and Recommended Countermeasures 2020; Pfleeger & Pfleeger 2012, 19-23.)

IoT:n turvallisuuden tutkimiseksi, voidaan IoT jakaa kerroksiin. Erilaisia malleja IoT:n jakamiseen on useita. Tässä esitetyn mallin mukaan IoT jaetaan viiteen eri kerrokseen havaintokerros, verkkokerros, käsittelykerros, sovelluskerros ja yrityskerros. (ks. kuvio 9) Havaintokerrokseen kuuluvat kaikki fyysiset laitteet ja sensorit, jotka keräävät tietoa ympäristöstään. Verkkokerrokseen kuuluvat tietoliikenneyhteydet laitteiden välillä. Käsittelykerroksessa dataa muun muassa muokataan, säilötään ja tutkitaan. Sovelluskerrokseen kuuluvat kaikki tietoliikenneprotokollat, sekä käyttöliittymät. Yrityskerroksessa määritellään säännöt, joiden mukaan koko järjestelmä toimii. Seuraavaksi käydään läpi tarkemmin näitä viittä eri tasoa ja turvallisuutta IoT-järjestelmässä niiden kautta. (Burhan, Rehman, Khan & Kim 2018; Sethi & Sarangi 2017.)

Kuvio 9 IoT:n jako viiteen kerrokseen.

3.1 Havaintokerros

Havaintokerrokseen kuuluvat kaikki järjestelmän fyysiset laitteet, jotka osallistuvat datan keräämiseen ja lähettämiseen. Ensimmäinen askel laitteiden ja koko järjestelmän turvaamiseksi on verkkoon yhdistettyjen laitteiden dokumentointi. Hyvään dokumentointiin kuuluu ainakin ajantasainen lista verkkoon yhdistetyistä laitteista, laitteiden valmistaja- ja mallitiedot, sarjanumerot, ohjelmistoversiot, laitekohtaiset asetukset. Dokumentointiin voidaan koota myös, mihin laitteita käytetään ja niiden riskialttius. Nämä tiedot auttavat mahdollisessa verkon segmentoinnissa, sekä palomuurin määrityksessä. (Burhan, Rehman, Khan & Kim 2018)

Laitteiden, kuten anturien ja tietoliikennelaitteiden, turvallisuuteen voidaan vaikuttaa paljon niiden sijoittelulla. Laitteiden tulisi olla helposti käsiteltävissä ja tarkastettavissa, mutta samalla suojassa ulkopuolisilta tekijöiltä. Sisätiloissa ulkopuolisten pääsyä käsiksi laitteisiin on helpompi estää, mutta ulkona olevien laitteiden koskemattomuutta uhkaavat niin luonto, kuin ihminenkin. Erilaisissa paikoissa olevat laitteet tarvitsevat erilaista suojausta. Esimerkiksi pölyisissä paikoissa laitteet tarvitsevat tiiviin suojan, joka estää pölyn pääsyn laitteen sisälle. Julkisilla paikoilla laitteet tarvitsevat järeämmän suojan ilkivallan estämiseksi. On myös tärkeää varmistaa, ettei laitteen sijoittelua muuteta. Varsinkin ulkona olevien laitteiden eheys olisi hyvä tarkistaa säännöllisin väliajoin. (Chaudhuri 2019.) Laitteiden valvonta ja sijoittelu estää myös hyökkääjää lisäämästä järjestelmään uusia laitteita. Hyökkääjän toimesta uuden laitteen lisäämistä kutsutaan fake nodeksi tai fake node injectioniksi. Uudella laitteella voidaan pyrkiä vaikuttamaan järjestelmän toimintaan tai varastamaan dataa järjestelmästä. (Burhan, Rehman, Khan & Kim 2018)

Ohjelmistopäivitykset ovat tärkeä osa laitteiden turvallisuutta. Päivityksillä voidaan parantaa laitteiden käytettävyyttä, korjata ohjelmistovikoja tai korjata havaittuja tietoturva-aukkoja. Laitteisiin tulisi tehdä ohjelmistopäivityksiä aina kun niitä on saatavilla. Useimmat IoT-laitteet eivät kuitenkaan ole suunniteltu jatkuvasti päivitettäviksi. Laitteita valitessa tulisi aina tarkistaa, onko päivittäminen mahdollista ja kauanko valmistaja aikoo tukea kyseisen mallin päivityksiä. Laitteet tulisi päivittää ennen niiden asentamista varsinkin, jos niiden päivittäminen jatkossa on haastavaa tai mahdotonta. (How to Secure IoT Devices in the Enterprise n.d.)

Useissa IoT-laitteissa valmiiksi asennettu salasana voi olla heikko ja sen saattaa löytää internetistä helposti. Salasanat tulisi vaihtaa ennen laitteiden käyttöönottoa ja uusille salasanoille tulisi olla ennalta määritellyt säännöt. Salasanojen tulisi olla tarpeeksi monimutkaisia ja pitkiä, sekä jokaisella laitteella tulisi olla eri salasana. (How to Secure IoT Devices in the Enterprise n.d.)

Laitteiden tilaa olisi hyvä seurata muutenkin, kuin tarkistamalla niiden eheys silmämääräisesti. Vaikka laitteet näyttävät ehyiltä, on niitä saatettu muokata. Hyvä tapa laitteiden seurantaan olisi laitteiden lähettämät raportit niiden toiminnasta, sekä hälytykset muutoksista tai virheistä. Joskus

tämä ei ole kuitenkaan mahdollista laitteiden heikon laskentatehon vuoksi. Toinen vaihtoehto on pilvessä toimiva sovellus, joka monitoroi laitteen lähettämää dataa ja hälyttää muutoksista käyttäjälle. Häiriön ilmetessä laitteen automaattinen uudelleenkäynnistyminen voi auttaa vian korjauksessa. (Chaudhuri 2019.)

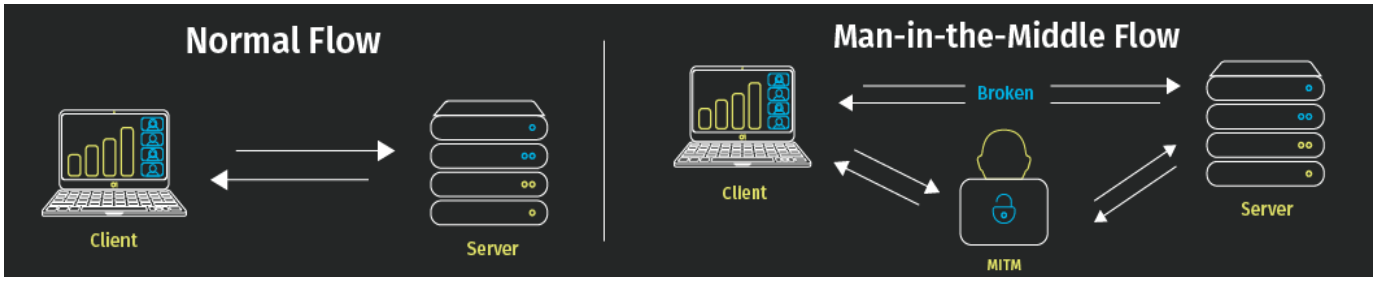
Jokaisen laitteen ohjelmistosta olisi hyvä olla mahdollisimman tuoreet varmuuskopiot. Jos turvallisuustoimet pettävät ja laite varastetaan tai sen ohjelmistoa muokataan, uuden laitteen asennusta tai vanhan laitteen palauttamista auttavat varmuuskopiot. (Chaudhuri 2019.)

3.2 Verkkokerros

IoT-ratkaisuissa monimutkaiset ja eri tekniikkaa käyttävät verkot voivat helposti luoda verkko-, turvallisuus- tai yhteysongelmia. Turvallinen verkkoyhteys on pakollinen osa turvallisen IoT-ratkaisun luomisessa. Jo IoT-ratkaisun suunnitteluvaiheessa on tärkeää määrittää käytettävän yhteyden suojaaminen. Langattomissa verkoissa on tärkeää valita turvallinen tiedonsiirtoprotokolla. Kiinteissä yhteyksissä palomuurien, tunkeutumisenestojärjestelmien ja vahvojen salausmekanismien käyttö on suositeltavaa. (Chaudhuri 2019.)

Laitteiden vähäinen laskenta- ja lähetysteho tekevät laitteista haavoittuvaisia ulkopuoliselle kuuntelulle ja häirinnälle. Yksi verkkokerrosta uhkaava hyökkäys on palvelunestohyökkäys. Palvelunestohyökkäyksessä hyökkääjä pyrkii estämään järjestelmän käytön. Yleensä hyökkäys toteutetaan ruuhkauttamalla verkko tarpeettomilla pyynnöillä tai muulla verkkoliikenteellä, jolloin käyttäjän pääsy järjestelmään estyy tai hankaloituu. (Burhan, Rehman, Khan & Kim 2018; Chaudhuri 2019.)

Yksi mahdollinen tapa suojaamattoman yhteyden kuunteluun, sekä väärän tiedon lähettämiseen on Man-in-the-Middle hyökkäys (Ks. kuvio). Yksinkertaistettuna hyökkäyksessä hyökkääjä pyrkii pääsemään viestinnän väliin ja esittää olevansa kumpikin viestinnän osapuoli. Tämä mahdollistaa kumpaankin suuntaan lähetetyn datan tutkimisen ja haitallisen tai väärän datan lähettämisen kummallekin osapuolelle. (Burhan, Rehman, Khan & Kim 2018; Man in the Middle (MITM) Attack n.d.)



Kuvio 10 Man-in-the-Middle hyökkäys(Man in the Middle (MITM) Attack n.d.).

3.3 Käsittelykerros

Käsittelykerroksessa kerätty ja verkkokerroksessa siirretty data muokataan sopivaan muotoon sitä käsittelevälle sovellukselle. Tällä kerroksella on myös mahdollista poistaa ylimääräinen data. Käsittelykerroksella käytetään väliohjelmistoja. Väliohjelmistolla mahdollistetaan järjestelmän eri osien kommunikointi, jotka eivät olisi muuten keskenään yhteensopivia. Tietoturvan kannalta tärkeää käsittelykerroksen ohjelmistoissa on käyttäjien todennus ja käyttöoikeuksien valvonta. (Burhan, Rehman, Khan & Kim 2018; Moné 2018.)

Yleinen käsittelykerrokseen kohdistuva hyökkäys pyrkii ylikuormittamaan väliohjelmiston ylimääräisellä datalla. Sama ylikuormittava vaikutus voi johtua myös palvelunestohyökkäyksestä verkkokerrosta kohtaan. Käsittelykerros voi myös ylikuormittua havaintokerrokselle kohdistuvasta hyökkäyksestä. Esimerkiksi, jos hyökkääjä pyrkii kuluttamaan laitteiden akkua lähettämällä lyhyellä aikavälillä paljon dataa. Väliohjelmat ovat myös haavoittuvaisia haittaohjelmille. (Burhan, Rehman, Khan & Kim 2018)

3.4 Sovelluskerros

Sovelluskerrokseen kuuluvat kaikki käytettävät sovellukset, tietoliikenneprotokollat ja käyttöliittymät. Järjestelmän käyttäjä on vuorovaikutuksessa koko järjestelmän kanssa sovelluskerroksen kautta.

Tietoliikenneprotokollat ovat erittäin tärkeä osa IoT-järjestelmää. Ne mahdollistavat kaiken viestinnän IoT-laitteiden, sekä IoT-laitteiden ja pilvessä olevien sovellusten välillä (Nebbione & Calzarossa 2020, 3). Sovelluskerros perustuu tavallisesti HTTP-protokollaan, mutta sen käyttö voi olla ongelmallista IoT-toteutuksissa vähäisen laskutehon vuoksi (Sethi & Sarangi 2017). Tätä varten on kehitetty HTTP:tä kevyempiä, IoT:ta varten suunniteltuja protokollia. Yksi kevyempi ratkaisu on Message Queue Telemetry Transport (MQTT). MQTT on laajasti IoT-ratkaisuissa käytetty protokolla. Se on yksinkertainen, kevyt ja suunniteltu käytettäväksi IoT-ratkaisuissa, joissa laskentatehon ja tietoliikenneyhteyden kapasiteetin säästäminen on tärkeää. MQTT tukee useita eri todennus mekanismeja, sekä Transport Layer Security (TLS) salausprotokollaan perustuvaa salausta. Koska MQTT ei itsessään sisällä salausta, on se ilman TLS:än käyttöä haavoittuvainen esimerkiksi Man-in-the-Middle hyökkäykselle. (Nebbione & Calzarossa 2020, 3).

Käyttöliittymät voivat olla haavoittuvaisia monille samoille hyökkäyksille, kuin tavalliset verkkosivut. Yksi tällainen hyökkäys on Cross-site scripting (XSS) hyökkäys. (Burhan, Rehman, Khan & Kim 2018) Hyökkäyksessä hyökkääjä pääsee syöttämään ohjelmakoodia sivulle ja näin esimerkiksi muokkaamaan sitä. Hyökkäykseltä voi suojautua oikeanlaisella HTML-koodilla. Hyökkäyksen estoa varten on myös olemassa ohjelmointikieleen sisäänrakennettuja funktioita ja kirjastoja. (Kristen n.d.)

Kun IoT-järjestelmän sovellukset sijaitsevat pilvessä, järjestelmän turvallisuuteen vaikuttaa myös pilvialustan turvallisuus. Esimerkiksi Microsoftin Azure-pilvipalvelu on julkinen pilvialusta, joka sisältää palvelut IoT-järjestelmän toteuttamiseksi, sekä pilvipohjaisten sovellusten kehittämiseksi. Azure sisältää useita sisäänrakennettuja ominaisuuksia, jotka auttavat ylläpitämään järjestelmän turvallisuutta. Azure sisältää muun muassa mahdollisuuden sovellusten haavoittuvuuksien tarkistamiseen, liikenteen salaamiseen verkkojen välillä, sekä verkon käytön valvontaan ja rajoittamiseen. Azure mahdollistaa myös yrityskerroksella määriteltyjen salasanakäytäntöjen käyttöönoton. (Introduction to Azure security 2022.)

3.5 Yrityskerros

Yrityskerroksella määritellään koko IoT-järjestelmän toiminta ja tarkoitus. Tällä kerroksella otetaan käyttöön ratkaisua käyttävän tai kehittävän organisaation säännöt ja käytännöt. Tarkoituksena on datan eheyden, saatavuuden ja luottamuksellisuuden ylläpitäminen. Yrityskerrokseen kuuluu myös tuotteen tutkiminen ja kehittäminen paremmaksi ja turvallisemmaksi. Yrityskerros ei välttämättä ole suoraan hyökkäyksen kohteena, mutta sekin voi sisältää haavoittuvuuksia. Yrityskerroksen haavoittuvuuksia voivat olla esimerkiksi heikot salasanakäytännöt, vääränlainen koodi ohjelmoijalta tai liian heikkojen salausalgoritmien käyttö. (Burhan, Rehman, Khan & Kim 2018)

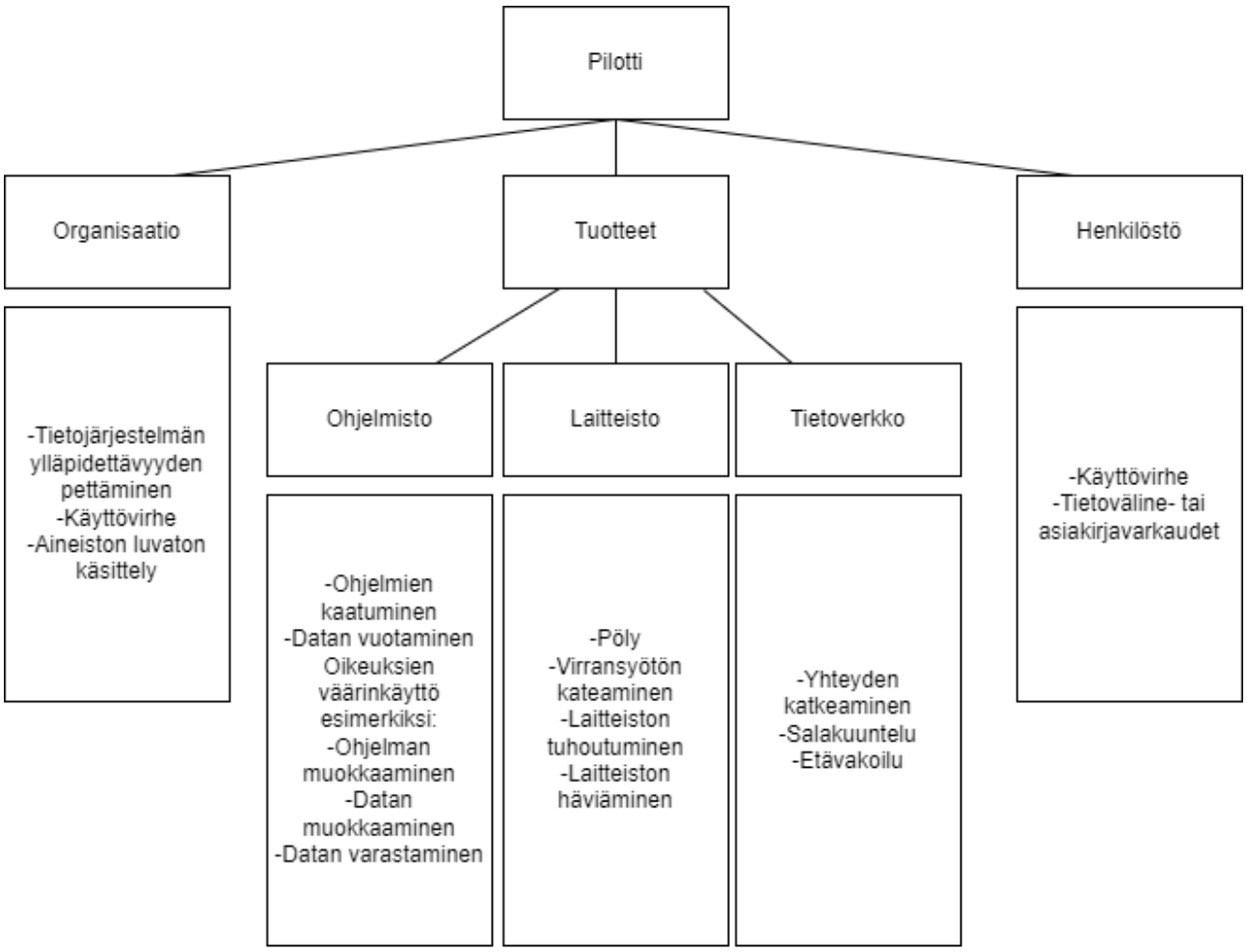
3.6 Riskienhallinta

Riskinhallinnalla voidaan edesauttaa IoT-järjestelmän ja sitä käyttävän organisaation toimintaa, sekä turvallisuutta. Riskienhallinnan tulisi olla jatkuva prosessi, joka alkaa jo ennen järjestelmän käyttöönottoa ja jatkuu koko järjestelmän eliniän. Riskienhallinnan tavoitteena on ainakin tunnistaa järjestelmää tai organisaatiota koskevat riskit, arvioida sitä koskevien riskien suuruus, sekä löytää sitä uhkaavat tietoturva-aukot. Riskien tunnistamisen jälkeen voidaan sopia toimintamalleja, jotka ennalta ehkäisevät tai pienentävät riskit hyväksyttävälle tasolle. Riskienhallintaan on olemassa lukuisia eri standardeja, mutta organisaatioiden monimuotoisuuden vuoksi, niitä ei aina voida suoraan soveltaa. Organisaation on löydettävä toimintaympäristöön, sekä organisaation sääntöihin sopiva toimintamalli. (SFS-ISO/IEC 27005:2018, 7-9.)

Riskianalyysi auttaa riskien luonteen ja suuruuden tunnistamisessa. Riskianalyysissä tunnistetaan riskien todennäköisyys tapahtua ja niiden vaikutus järjestelmän tai organisaation toimintaan. Kuten koko riskienhallinta, myös riskianalyysin yksityiskohdat ja laajuus voi vaihdella riippuen esimerkiksi aiemmista häiriöistä tai suojeltavan omaisuuden kriittisyydestä. Riskianalyysi voi olla laadullinen tai määrällinen. Laadullisessa riskianalyysissä riskien, sekä mahdollisten seurausten suuruusluokasta käytetään esimerkiksi pieni, keskitaso ja suuri asteikkoa. Tällainen asteikko on helppo ymmärtää, mutta se ei ole yhtä tarkka, kuin määrällisessä riskianalyysissä käytettävä numeraalinen asteikko. Laadullista riskianalyysiä tulisi käyttää vain, jos kyseessä on alustava

riskianalyysi tai käytettävissä ei ole tarpeeksi numeerista aineistoa tai resursseja määrällistä riski-analyysiä varten. (SFS-ISO/IEC 27005:2018, 18.)

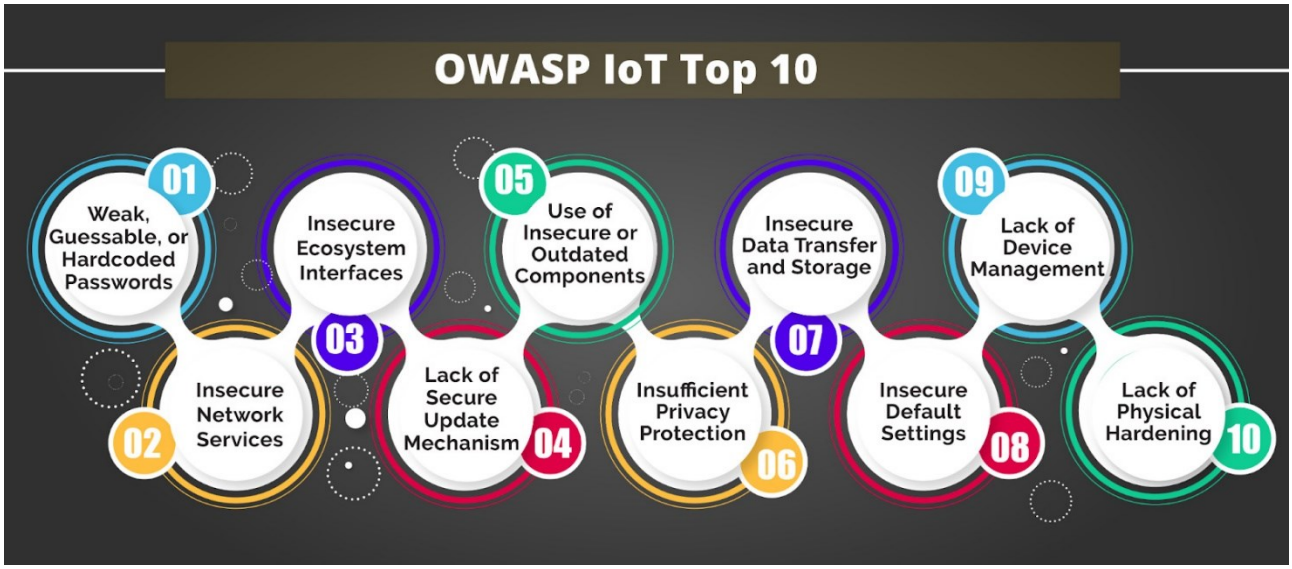
Uhkien tunnistamisen apuna voidaan käyttää esimerkiksi uhkapuuta. Uhkapuussa organisaation osat jaetaan eri ”oksille”, jolloin uhkia voidaan miettiä pienempinä ryhminä. Kuviossa 10 esitetty uhkapuu, jossa suojeltava kohde on tässä opinnäytetyössä tutkittava pilotti. Uhkapuussa tutkittava kohde jaetaan osiin, jotka auttavat löytämään niihin kohdistuvat uhat. (Hautamäki 2021.)



Kuvio 11 Esimerkki uhkapuusta

3.7 OWASP TOP 10

OWASP Internet of Things-projekti alkoi vuonna 2014. Tavoitteena oli auttaa kehittäjiä, valmistajia, yrityksiä ja kuluttajia IoT-järjestelmien käyttämisessä ja kehittämisessä. Vuonna 2018 OWASP julkaisi Top 10 listan asioista, joita tulisi välttää IoT-järjestelmien kehittämisessä ja käyttämisessä (ks. kuvio 11). Usein erillisten riski, uhka, haavoittuvuus listoista poiketen OWASP:in tarkoitus oli luoda yksi lista, jossa ovat asiat, joita IoT-järjestelmien turvallisuuden kanssa tulisi välttää. Listaa perustuu haavoittuvuuksien hyödynnettävyyteen, vakavuuteen ja havaittavuuteen, sekä mahdollisiin vaikutuksiin. (Basatwar 2021; OWASP Internet of Things Top 10 2018.)



Kuvio 12 Tärkeimmät haavoittuvuudet (Basatwar 2021).

Tärkeysjärjestyksessä heikkoudet olivat seuraavat.

Heikot, arvattavat tai ennalta asetetut salasanat.

Valmistajien tulee kiinnittää huomiota salasana asetuksiin, ennen laitteiden julkaisua. Voi olla, että laitteen salasanaa ei voi vaihtaa ollenkaan tai käyttäjä ei vaihda sitä vaikka voisi. Murrettu salasana voi myös asettaa muut samanlaiset laitteet vaaraan, jos niissä kaikissa on sama salasana.

Epäturvalliset verkkopalvelut.

Laitteiden väliseen kommunikointiin käytettävät verkkopalvelut voivat uhata koko järjestelmän turvallisuutta ja eheyttä. Internettiin yhdistettynä nämä voivat mahdollistaa luvattoman pääsyn järjestelmiin etänä, sekä tietovuodon.

Epäturvalliset käyttöliittymät.

IoT-järjestelmissä voi olla useita erilaisia käyttöliittymiä, jotka mahdollistavat käyttäjälle sulavan kokemuksen. Puutteellinen käyttäjän todennus, huono salaus ja tietojen suodatus voivat kuitenkin vaarantaa järjestelmän turvallisuuden.

Turvallisten päivittämistapojen puute.

Laitteiden turvallinen päivittäminen on mahdotonta ilman laiteohjelmiston varmistusta, suojattua tiedon siirtoa, rollback:in estoa ja ilmoituksia turvallisuuspäivityksistä.

Epäturvallisten tai vanhentuneiden komponenttien käyttö.

Kolmannen osapuolen laitteiden tai ohjelmistojen käyttö voi vaarantaa koko järjestelmän. Varsinkin IIoT-ratkaisut kärsivät näistä komponenteista, joita on vaikea päivittää tai ylläpitää. Kyseiset haavoittuvuudet voivat helposti mahdollistaa kyberhyökkäyksen ja uhata koko järjestelmän toimintaa.

Riittämätön yksityisyydensuoja.

IoT-laitteet täytyy usein säilöä dataa toimiakseen. Kuitenkin laitteet usein eivät ole tarpeeksi hyvin suunniteltuja datan turvalliseen säilömiseen. Tämä voi johtaa kriittisen datan menetykseen hyökkäyksen sattuessa. Myös laitevalmistajien tietokannat voivat olla alttiita hyökkäyksille.

Epäturvallinen datan siirto ja varastointi.

Salauksen puute dataa siirtäessä, käsiteltäessä tai varastoitaessa mahdollistaa datan joutumisen vääriin käsiin. Salaus on ehdoton varsinkin, jos kyseessä on arkaluontoista dataa.

Laitehallinnan puute, jolla tarkoitetaan kaikkien laitteiden tehokkaan suojaamisen puutetta.
Riippumatta laitteiden määrästä tai koosta, joka ikinen täytyy olla yhtä tehokkaasti suojattu. Heikko lenkki järjestelmässä luo useita eri haavoittuvuuksia.

Turvattomat, ennalta asetetut asetukset.
Nämä voivat altistaa järjestelmän useille tietoturvaongelmille. Esimerkiksi myös aikaisemmin mainitut ennalta määrätyt salasanat, vanhojen komponenttien käyttö ja päivitysten vaikeuttaminen voivat kuulua näihin asetuksiin.

Fyysisen koventamisen puute voi mahdollistaa koko järjestelmän kaappaukseen.
Laitteisiin käsiksi pääsevä ihminen voi esimerkiksi avata itselleen etäyhteyden järjestelmään tai aiheuttaa tuhoa viemällä laitteesta muistikortin.

4 Tutkimuksen kohteet

Tutkimuksen kohteena ovat kaksi eri teknologioilla toteutettua IoT-järjestelmää. Tässä kappaleessa käydään läpi tarkemmin tutkittavia pilotteja ja erityisesti niiden käyttämiä laitteita, tietoliikenneyhteyksiä ja sovelluksia.

4.1 Pilotti Sammakkokangas

Sekajätteen itsestään syttyminen aiheutuu biojätteen hajotessa jätekasan sisällä. Syttymistä voi olla vaikea ennustaa sekä sammuttaa. Jätepalo on suuri ympäristöriski ja voi aiheuttaa merkittäviä taloudellisia vahinkoja. Sammakkokankaan jätekeskuksen kanssa yhteistyössä kehitetty IoT-ratkaisun tarkoituksena on tunnistaa, ennakoida ja ehkäistä sekajätteen itsestään syttymistä (ks. kuvio 12). Kyseistä ratkaisua voidaan käyttää myös muissa sellaisissa ympäristöissä, jossa on olemassa itsesyttymisvaara. (Väänänen 2020).

Kuvio 13 Järjestelmän kuvaus (kuva Heli Sutinen).

Tässä ratkaisussa anturit mittaavat jätekasasta sen lämpötilaa, kosteutta, sekä vapautuvien kaasujen kuten metaanin, hiilidioksidin ja hiilimonoksidin määrää. Lisäksi ratkaisuun kuuluu jätekasaa kuvaava kamera. Kerättävä tieto lähetetään Azuren pilvipalvelussa toimivaan Thingsboard-alustaan, käyttäen mobiilidataa. Thingsboardista kerättyä tietoa voidaan seurata ja sen perusteella voidaan luoda ennuste jätekasan syttymisestä. (Väänänen 2020).

Jätesiiloissa sijaitsevat mittausanturit ovat yhteydessä yhdyskäytävänä toimivaan Linux tietokoneeseen Raspberry Pi:hin Wi-Fi:n avulla. Wi-Fi-verkko on rakennettu käyttäen Arduino Uno WiFi:ä. Se kommunikoi langattomasti antureiden, sekä yhdyskäytävän kanssa. Siilojen ulkopuolella

sijaitsevat anturit, joita käytetään vertailumittauksiin, ovat yhdistetty suoraan yhdyskäytävään. (Väänänen 2020).

4.2 Pilotti VAPO

VAPO:n kanssa yhteistyössä kehitetty IoT-ratkaisu seuraa turpeen keräystä ja aumaan ajoa Vapo Oy:n turvetuotantoalueilla Keski-Suomessa. Seurantajärjestelmällä on reaaliaikaisen turvetuotanto määrän seuraamisen lisäksi mahdollista ajokirjan automaattinen päivittäminen. Kyseistä ratkaisua voidaan käyttää myös esimerkiksi puunkorjuun ja varastoinnin seuraamisessa. (Hautamäki 2020.)

Kokoojavaunun kerätessä turvetta, lähetetään paikannus dataa pilvipalveluun. Vaunun luukkujen avautuessa, sijaintitietoa tarkastellaan pilvessä olevassa sovelluksessa ja jos luukut ovat auenneet auman kohdalla, rekisteröidään tapahtuma lastin purkamisena aumaan. (Hautamäki 2020.)

Pilotissa käytettiin kahta eri ratkaisua. Kehittyneemmässä ratkaisussa käytettiin yhdyskäytävänä Arduino Uno mikrokontrolleria. Järjestelmässä dataa keräävät paineanturi ja merkkilamppu. Paineanturilla tunnistetaan, onko vaunun luukku kiinni vai auki. Merkkilampulla seurataan, onko vaunu tyhjä vai täysi. Kerättävä tieto lähetetään mobiilidataa käyttäen Thingsboard-alustaan Azuren pilveen. (Hautamäki 2020.)

Kevyemmässä ratkaisussa käytetään kuluttajille suunnattua ”trakkeriä”. Trakkeri alkaa lähettämään paikannustietoa vaunun liikkuessa. Liikkeelle lähtö tunnistetaan inertiasensorilla. Liikkeelle lähdön tunnistamisen jälkeen trakkeri herää deep sleep tilasta ja lakaa lähettämään paikannus dataa pilveen. Trakkeri tunnistaa vaunun luukkujen aukeamisen sisäänrakennetulla magnetometrillä ja lähettää paikannustiedon pilveen, johon tyhjennyspaikka rekisteröidään. Data trakkeristä pilveen lähetetään käyttäen LORA-verkkoa. Myös tässä ratkaisussa käytetään Azuren pilvipalvelua ja Thingsboard alustaa. (Hautamäki 2020.)

5 Tulokset

Tuloksissa käsitellään opinnäytetyön tavoitteiden mukaisesti eÄlytelli-hankkeen pilottien haavoittuvuuksia. Haavoittuvuuksia pyritään löytämään käyttämällä aikaisemmin mainittua kerroksiin jakoa. Jokaisen kerroksen kohdalla käydään läpi kummankin pilotin haavoittuvuuksia, sekä lopussa vertaillaan pilottien turvallisuutta. Haavoittuvuuksien havainnointi perustuu kirjallisuudessa esitettyihin haavoittuvuuksiin, eikä niitä testata käytännössä.

5.1 Havaintokerros

Kummankin pilotin laitteet ovat ulkona ja vartioimattomana, joka tekee niistä haavoittuvaisia olosuhteiden muutoksille ja ilkivallalle. Laitteita ja niiden eheyttä ei tarkisteta säännöllisesti, eikä ne lähetä dataa omasta toiminnastaan. Vapon pilotin laitteet altistuvat turvevaunujen kyydissä jatkuvasti hienojakoiselle pölylle, kosteudelle, lämpötilan vaihtelulle, sekä tärinälle. Ne ovat suojattu pölytiiviillä kotelolla, joka ei kuitenkaan suojaa niitä ilkivallalta tai muuntelulta. Muuntelun lisäksi akkukäyttöisten laitteiden virtaa on mahdollista kuluttaa tahallaan, esimerkiksi lähettämällä dataa tai häiritsemällä laitteiden lepotilaa. Akuttomissa ratkaisuissa, kuten sammakkokankaan pilotissa, laitteet ovat riippuvaisia verkkovirrasta ja niiden toiminta lakkaa sähkökatkon sattuessa. Piloteissa eri laitteita on vain muutamia, mutta ne ovat hyvin pitkälti eri osista muokattuja ja rakennettuja kokonaisuuksia, jotka ovat vaikeita korvata tai korjata hajoamisen tai varkauden tapahtuessa, sekä vaikeita päivittää tulevaisuudessa. Kaikista laitteista ei ole valmiiksi olemassa samanlaista varalaitetta. Uuden laitteen lisääminen järjestelmään hyökkääjän toimesta on mahdollista.

Haavoittuvuudet:

-Fyysisen suojan puutteellisuus
-Laitteita ei tarkisteta säännöllisesti / ne eivät ilmoita tilastaan
-Yhteen virtalähteeseen luottaminen
-Huono päivitettävyys
-Varalaitteiden puute
-Fake node

5.2 Verkkokerros

Verkkokerroksella kummassakin pilotissa on useita eri haavoittuvuuksia. Vapon kehittyneemmässä pilottiversiossa, sekä Sammakkokankaan pilotissa käytetyt Wi-Fi- ja 4G-yhteydet eivät ole täysin turvallisia. Wi-Fi-yhteyden salaus on mahdollista murtaa ja sitä voidaan myös häiritä. Myös 4G-yhteyttä vastaan on olemassa useampia tunnettuja hyökkäyksiä. Vapon kummassakin ratkaisussa on käytössä GPS-paikannus, joka on myös altis häirinnälle. GPS-yhteyden häirintä voi myös johtaa yksinkertaisemmassa ratkaisussa käytettävän laitteen turhaan heräämiseen akunsäästötilasta, jolla taas voidaan vaikuttaa akun kestoon. Yksinkertaisemmassa ratkaisussa käytetyssä LORA-yhteydessäkin omat haavoittuvuudet. LORA:n kuuluvuus on vaihteleva, sekä sitä pystytään häiritsemään. LORA on myös altis palvelunestohyökkäyksille (Denial of Service, DoS), joissa kaapattua pakettia lähetetään uudestaan ja uudestaan vastaanottajalle, estäen tällöin oikean viestinnän. LORA-yhteys on haavoittuvainen myös muille hyökkäyksille, jotka kuitenkin ovat liian monimutkaisia tai vaikeita toteuttaa saatavaan hyötyyn, eli turpeen keräysdataan verrattuna. Datan lähetyksen estäminen olisi helpompaa esimerkiksi rikkomalla laitteet. Tulevaisuudessa, jos pilotteja kehitetään ja lähetettävä data on arkaluontoisempaa tai sen perille meneminen on tärkeämpää, tulee LORA-yhteyteen kiinnittää enemmän huomiota. LORA-yhteys tässä ratkaisussa käyttää yhdensuuntaista viestintää, eli tiedon perille menosta ei ole ikinä varmuutta. Virheen tai kuuluvuusongelman sattuessa dataa ei siis lähetetä uudelleen. Viesti sisältää kuitenkin laskurin, jonka avulla huomataan välistä mahdollisesti puuttuvat viestit.

Haavoittuvuudet:

-Tietoliikenneratkaisut: Wi-Fi, LORA, 4G
-Kuuluvuuden vaihtelu
-Yksisuuntainen liikennöinti
-GPS-paikannus
-Palvelunestohyökkäykset

5.3 Käsittelykerros

Kummassakin pilotissa on käytössä väliohjelmia, joilla dataa muokataan pilvessä. Näitä väliohjelmia on mahdollista ylikuormittaa suurella määrällä dataa, ja ne voivat ylikuormittua myös palvelunestohyökkäyksen sattuessa. Väliohjelmat ovat myös haavoittuvaisia ohjelman muuntamiselle ja haittaohjelmille. Vapo pilotissa on käytössä Node-RED väliohjelma, joka vastaanottaa, käsittelee ja lähettää eteenpäin LORA-yhteydellä saapuvia viestejä. Node-RED saa uusia tietoturvapäivityksiä, mutta ohjelmaversiosta riippuen siitä löytyy erilaisia haavoittuvuuksia. Esimerkiksi tietyssä versiossa on Cross-site scripting-hyökkäyksen mahdollistava haavoittuvuus.

Haavoittuvuudet:

-Väliohjelman ylikuormitus

-Ohjelmien muokkaus mahdollista

-Haittaohjelmat

-Palvelunestohyökkäykset

-Node-RED haavoittuvuudet

5.4 Sovelluskerros

Sovelluskerrokseen kuuluva Azure-pilvipalvelu on itsessään hyvin turvallinen, mutta sen väärinkäytön kautta voi syntyä isoja tietoturva-aukkoja. Kummassakin pilotissa käytössä olevan pilvipalvelun kautta on mahdollista vuotaa tietoa ulkopuolisille. Väärät asetukset datan säilönnässä ja käsittelyssä, sekä datan säilöminen sitä salaamatta ovat isoimmat uhat. Jos hyökkääjä pääsisi kirjautumaan sisään pilvipalveluun, pilvipalvelussa olisi mahdollista muokata sovelluksia, varastaa dataa tai lisätä haittaohjelmia. Hyökkääjän tekemiä muutoksia ei välttämättä huomattaisi heti yrityskerroksen haavoittuvuuksien takia.

Haavoittuvuudet:

-Datan säilöminen/käsittely

-Datan salaamisen puute

-Tunnistus- ja todennusmekanismien puute

-Ohjelmien muuntaminen

-Haittaohjelmat

5.5 Yrityskerros

Yrityskerroksen haavoittuvuudet ovat erittäin monimuotoiset ja koska tutkittavat kohteet ovat pilotteja, niiden hallinta puuttuu kokonaan. Pilotti vaiheessa yrityskerroksen haavoittuvuudet eivät ole vielä niin tärkeitä, mutta jos ratkaisut otetaan käyttöön johonkin yritykseen, on otettava silloin huomioon sen yrityksen tieturvapolitiikka, tietoturvariskien hallintajärjestelmä ja sen kautta luodut ohjeistukset ja säännöt. Tällä hetkellä pilottien yrityskerroksen haavoittuvuuksia ovat esimerkiksi puuttuvat yhtenäiset salasanakäytännöt, kaikkien ratkaisujen suunnitelmat ja yksityiskohdat ovat internetissä kaikkien saatavilla, pilotteihin osallistuville henkilöille ei ole järjestetty yhtenevää koulutusta datan käsittelystä tai tietoturvan merkityksestä hankkeissa.

Haavoittuvuudet:

-Lähes kaikki järjestelmien tiedot julkisesti saatavilla

-Puutteellinen tietoturvapolitiikka

-Puutteellinen tietoturvan hallintajärjestelmä

-Vajavainen riskienhallinta

-Puuttuvat tai alimitoitetut tietoturvamekanismit

-Puutteellinen jatkuvuuden hallinta

-Henkilöstön osaamisen tason puutteellisuus

5.6 Yhteenveto

Piloteista löytyi reilusti erilaisia haavoittuvuuksia. Löydetyt haavoittuvuudet havainnollistettu taulukossa 1. Eniten haavoittuvuuksia löytyi yrityskerrokselta. Kummankin pilotin takana on sama hanke ja sitä kautta samat yrityskerroksen säännöt, joten haavoittuvuudetkin olivat samat

kummassakin pilotissa. Kuten jo aikaisemmin mainittu tämä ei kuitenkaan ole tärkeä kerros ratkaisujen ollessa pilotti vaiheessa.

Taulukko 1 Piloteista löytyneiden haavoittuvuuksien määrä.

	Pilotti Vapo	Pilotti Sammakkokangas	Yhteensä
Havaintokerros	6	6	12
Verkkokerros	8	2	10
Käsittelykerros	2	2	4
Sovelluskerros	5	5	10
Yrityskerros	7	7	14
Yhteensä	28	22	50

Seuraavaksi eniten haavoittuvuuksia löytyi havaintokerrokselta. Havaintokerroksen haavoittuvuudet olivat myös samat kummallakin pilotilla. Havaintokerroksen haavoittuvuudet johtuivat enimmäkseen siitä, että pilottien laitteet ovat ulkona valvomattomina ja kyseessä on useista osista rakennetut ainutlaatuiset kokonaisuudet. Tälläkin kerroksella on siis selkeästi havaittavissa ratkaisujen pilottiluonne.

Seuraavaksi eniten haavoittuvuuksia löytyi verkko- ja sovelluskerroksilta. Verkkokerroksen haavoittuvuuksien määrässä näkyi selkeästi Vapon pilotissa käytetyt LORA ja GPS. Tässä vertailussa on otettava huomioon, että Vapon pilotissa on kaksi eri ratkaisua. Tällä kerroksella haavoittuvuudet voisivat olla lähes samat myös pidemmälle kehitetyissä versioissa, sillä piloteissa käytetyt tietoliikenneyhteydet ovat erittäin yleisiä.

Sovelluskerroksella pilottien välillä ei ollut eroa. Kummassakin pilotissa on käytössä sama pilvipalvelu ja siellä toimivat sovellukset, joten myös haavoittuvuudet ovat samat. Piloteissa käytetyt sovellukset ovat yleisiä, joten kerroksen ohjelmiin liittyvät haavoittuvuudet voisivat olla lähes samat

myös kehittyneemmissä ratkaisuissa. Sovellusten turvallisuudesta vastaa sovelluksien kehittäjät, joten yleisiä sovelluksia käytettäessä ratkaisuiden suunnittelussa suurin huomio tulisi suunnata turvallisten sovelluksien valitsemiseen.

Käsittelykerroksella reilusti vähiten haavoittuvuuksia. Tämä ei välttämättä kerro kerroksen ylivoimaisesta turvallisuudesta, vaan kerroksen suppeudesta. Käsittelykerroksella ei ole muuta hyökkäyspinta-alaa, kuin muutama tietoa muokkaava ohjelma. Myös tällä kerroksella kummankin pilotin haavoittuvuudet olivat samat.

Tuloksista voi huomata, että käsittelykerrosta lukuun ottamatta kaikilta kerroksilta löytyi lähes yhtä paljon haavoittuvuuksia. Monet tuloksissa kuvatut haavoittuvuudet ylettyvät useille eri kerroksille ja ne ovat toisistaan riippuvaisia. Vapon pilotista löytyi hieman enemmän haavoittuvuuksia. Ero johtui verkkokerroksesta, sekä Vapon pilotissa käytetyistä kahdesta eri ratkaisusta. Haavoittuvuuksien lähes sama määrä pilottien välillä kertoo pilottien samankaltaisuudesta, sekä löydettyjen haavoittuvuuksien yleisyydestä erilaisten IoT-järjestelmien keskuudessa. Haavoittuvuuksien tarkastelussa tuli monesti esille ratkaisujen pilottimaisuus. Koska kyseessä on nimenomaan pilotit, eivät tuloksien haavoittuvuuksien määrä ollut yllätys. Useat haavoittuvuudet voisivat korjaantua, kun ratkaisut otettaisiin laajemmin käyttöön, sekä niistä vastaisi jokin yritys. Ottaen huomioon kyberhyökkäysten yleistymisen ja piloteista löydettyjen haavoittuvuuksien määrän, voidaan päätellä, että kyberturvallisuuden huomioon ottaminen uusia IoT-järjestelmiä suunniteltaessa tai pilottien jatkokehityksessä on erittäin tärkeää.

6 Johtopäätökset ja pohdinta

Opinnäytetyön tavoitteena oli tutkia yleisesti IoT-järjestelmiin kohdistuvia haavoittuvuuksia, sekä mitkä niistä ovat eÄlytelli-hankkeen JAMK:in pilotteihin kohdistuvia haavoittuvuuksia. Tavoite täytettiin yleisesti IoT-järjestelmiin kohdistuvien haavoittuvuuksien tutkimisella kerroksittain, sekä vertaamalla niitä pilotteihin. IoT-järjestelmiä koskevia haavoittuvuuksia löytyi lähes rajattomasti ja niistä pyrittiin rajaamaan tähän opinnäytetyöhön vakavimmat, sekä eniten tutkittavia pilotteja

koskevat. Kirjallisuuden avulla piloteista löytyi helposti useita haavoittuvuuksia, mutta osa jäi varmasti toteamatta. Paremman kuvan pilottien haavoittuvuuksista olisi saanut testaamalla niitä. Testeissä olisi voinut löytyä myös uusia haavoittuvuuksia. Opinnäytetyön isoimpia saavutuksia oli löytää kerroksittainen tapa, jolla IoT-järjestelmiä lähestyttiin. Kerroksista yrityskerros kuitenkin osoittautui pilotteja tutkiessa lähes hyödyttömäksi. Opinnäytetyön jatkokehitys vaatisi haavoittuvuuksien testaamisen lisäksi perusteellisemmat korjausehdotukset löydettyihin haavoittuvuuksiin, sekä paremman arvioinnin haavoittuvuuksien hyväksikäytön todennäköisyydestä.

Lähteet

Basatwar, G. 2021. Guide To OWASP IoT Top 10 For Proactive Security. Appsealing blogi. Julkaistu 11.5.2021. Viitattu 16.12.21. https://www.appsealing.com/owasp-iot-top-10/.

Bissel, K., Fox, J., LaSalle, R. & Cin, P. 2021. The state of cybersecurity resilience 2021. Accenture:n tutkimus kyberturvallisuudesta. Viitattu 3.4.2022. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf/.

Bissel, K., Lasalle, R. & Dal Cin, P. 2019. Ninth Annual Cost of Cybercrime Study. Accenturen tutkimus kyberrikoksien vaikutuksesta. Viitattu 3.4.2022. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf/.

Burhan, M., Rehman, R., Khan, B. & Kim, B. 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Artikkeli IoT:n kerros arkkitehtuurista ja niiden uhista. Viitattu. 21.11.2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453/.

Chang, W. & Wu, J. 2021. Fog/Edge Computing For Security, Privacy, and Applications. Springer. Viitattu 20.9.2021. https://janet.finna.fi, Ellibslibrary.

Chaudhuri, A. 2019. Internet of Things, for Things, and by Things. CRC Press. Viitattu 15.10.2021. https://janet.finna.fi, Skillsoft.

Cisco Annual Internet Report. 2020. Cisco:n tutkimus erilaisten tietoliikenneratkaisujen kehittymisestä. Viitattu 20.9.2021. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html/.

Crane, C. 2021. Re-Hashed: 27 Surprising IoT Statistics You Don't Already Know. SSL Store:n blogi. Julkaistu 17.2.2021. Viitattu 20.9.2021. https://www.thesslstore.com/blog/20-surprising-iot-statistics-you-dont-already-know/.

eÄlytelli-hanke. N.d. eÄlytelli-hankkeen verkkosivut. Viitattu 15.4.2021. https://ealytelli.fi/hanke/.

Gilchrist, A. 2017. IoT Security Issues. DEG Press. Viitattu 205.2021. https://ebookcentral-proquest-com.ezproxy.jamk.fi:2443/lib/jypoly-ebooks/reader.action?docID=4810138.

Hautamäki, J. 2020. Turpeen keräyksen reaaliaikaista seurantajärjestelmää kehitetään yhdessä VAPO:n kanssa. Viitattu 9.9.2021. https://blogit.jamk.fi/techtothefuture/2020/11/20/turpeen-kerayksen-reaaliaikaista-seurantajarjestelmaa-kehitetaan-yhdessa-vapon-kanssa/.

Hautamäki, J. 2021. Asset & Threat management Risk Analysis. Opettajan materiaalit. Jyväskylän ammattikorkeakoulu. Viitattu 16.12.2021.

Hautamäki, J. 2021. Digitalisaation murros: Teollinen internet. Opettajan materiaalit. Jyväskylän ammattikorkeakoulu. Viitattu 12.2.2021

Hertog, B. 2019. Different Ways to Connect IoT Devices to Transmit and Receive Data. Embedded AMS blogikirjoitus. Viitattu 3.5.2021. https://embeddedams.nl/different-ways-to-connect-iot-devices-to-transmit-and-receive-data/.

How to Secure IoT Devices in the Enterprise. N.d. Palo Alto Networks:in artikkeli yritysten IoT-laitteiden suojaamisesta. Viitattu 21.11.2022. https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise/.

Introduction to Azure security. 2022. Artikkeli Azure-pilvipalvelun turvallisuudesta. Viitattu 15.2.2022. https://docs.microsoft.com/en-us/azure/security/fundamentals/overview/.

IoT Attacks, Hacker Motivations, and Recommended Countermeasures. 2020. EMnify:n selvitys erillaisista hyökkääjistä. Viitattu 15.12.2021. https://www.iotforall.com/iot-attacks-hacker-motivation/.

IoT Signals. 2021. Microsoft:in tutkimus IoT:n kehittymisestä. Viitattu 15.10.2021. https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT%20Signals_Edition%202_English.pdf/.

Kelly, M. 2020. What is an iot gateway. Artikkeli yhdyskäytävän toiminnasta. Viitattu 3.5.2021. https://www.lanner-america.com/blog/what-is-an-iot-gateway/.

Kristen, S. N.d. Cross Site Scripting (XSS). Artikkeli XSS-haavoittuvuuksista. Viitattu 14.2.2022. https://owasp.org/www-community/attacks/xss/

Kundhavai, K & Sridevi, S. 2016. IoT and Big Data- The Current and Future Technologies: A Review.

International Journal of Computer Science and Mobile Computing, 5, 1, 10-14. Viitattu 10.5.2021.

https://www.ijcsmc.com/docs/papers/January2016/V5I1201604.pdf/.

Kuukka, A. N.d. LoRaWAN-teknologia. Digitan verkkosivut. Viitattu 15.5.2021. https://www.digita.fi/etusivu/palvelut-yrityksille/digitan-iot-palvelut/lorawan-teknologia/.

Man in the Middle (MITM) Attack. N.d. Julkaisu Man-in-the-middle-hyökkäyksistä. Viitattu 21.11.2021. https://www.veracode.com/security/man-middle-attack/.

Marr, B. 2018. What is Industry 4.0? Here's A Super Easy Explanation For Anyone. Forbes 2.9.2018. Viitattu 20.4.2021. https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/?sh=5ff381949788.

Moné, L. 2018. Internet of Things: Middleware. Artikkeli IoT-järjestelmien väliohjelmista. Viitattu 10.1.2021. https://www.leanix.net/en/blog/internet-of-things-middleware/.

Nebbione, G & Calzarossa, M. 2020. Security of IoT Application Layer Protocols: Challenges and Findings. Tutkimus sovelluskerroksen protokollista. Viitattu 15.1.2022 https://www.researchgate.net/publication/340007148_Security_of_IoT_Application_Layer_Protocols_Challenges_and_Findings/fulltext/5e72e1bba6fdcc37caf63d93/Security-of-IoT-Application-Layer-Protocols-Challenges-and-Findings.pdf/.

OWASP Internet of Things Top 10. 2018. OWASP:in lista tärkeistä haavoittuvuuksista. Viitattu 16.12.2021. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf/.

Padhi, P & Charrua-Santos, F. 2021. Tutkimus 6G-yhteyden vaikutuksesta IoT:hen. Viitattu 15.10.2021. https://www.mdpi.com/2571-5577/4/1/11/pdf/.

Pfleeger, C. & Pfleeger, S. 2012. Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach. Pearson.

Ray, J., Marshall, H., Boyce, R., De Sousa, V. & Foster, C. 2021. Cyber Threat Intelligence Report.

Accenturen tutkimus kyberuhista. Viitattu 3.4.2022. https://www.accenture.com/_acnmedia/PDF-173/Accenture-Cyber-Threat-Intelligence-Report-Vol-2.pdf/.

Segarra, J. 2022. 4G is the Most Common Cellular Connectivity for IoT. SORACOM blogi. julkaistu 12.1.2022. Viitattu 15.2.2022. https://www.soracom.io/blog/4g-is-the-most-common-cellular-connectivity-for-iot/.

Sethi, P. & Sarangi, S. 2017. Internet of Things: Architectures, Protocols, and Applications. Artikkeli erilaisista IoT-tekniikoista. Viitattu 21.11.2021. https://www.hindawi.com/journals/jece/2017/9324035/#related-articles/.

SFS-ISO/IEC 27005:2018. Ohjeistuis tietoturvariskien hallintaan. Aihealueet: Turvallisuustekniikat, Tietoturvariskien hallinta. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.12.2018. Viitattu 14.2.2022. https://janet.finna.fi/, SFS Online.

Supon vuosikirja 2021: Suomalaisten on varauduttava Venäjän vaikuttamisyrityksiin Nato-keskustelun aikana. 2022. Supon tiedote 29.3.2022. Viitattu 10.4.2022. https://supo.fi/-/supon-vuosikirja-2021-suomalaisten-on-varauduttava-venajan-vaikuttamisyrityksiin-nato-keskustelun-aikana/.

Väänänen, O. 2020. Data-analytiikasta apua sekajätteen itsesyttymisen ennakointiin ja tunnistamiseen. Viitattu 9.9.2021. https://blogit.jamk.fi/techtothefuture/2020/04/14/data-analytiikasta-apua-sekajatteen-itsesyttymisen-ennakointiin-ja-tunnistamiseen/.

Yritysjohdon opas IoT:n ja teollisen internetin hyödyntämiseen. N.d. Elisan ja Quvan laatima opas. Viitattu 3.5.2021 https://quva.fi/site/attachments/yritysjohdon_opas_IoT_ja_teollisen_internetin_hyodyntamiseen.pdf.