Joonas Luukkonen

ÄLYKODIN IOT-LAITTEIDEN KYBERTURVALLISUUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Luukkonen, Joonas
Älykodin IoT-laitteiden kyberturvallisuus.
Jyväskylä: Jyväskylän yliopisto, 2020, 28 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Kyppö, Jorma

Erilaisten laitteiden määrä internetissä on jatkuvassa nousussa. Näille laitteille on suurta kysyntää, ja niiden hyödyt ovat selkeitä tietyille käyttäjäryhmille. Osa näistä laitteista on osana älykotia, tehden asukkaiden arjesta helpompaa sekä turvallisempaa. Näihin laitteisiin liittyy kuitenkin erilaisia kyberturvauhkia, ja tämän tutkielman tarkoituksena on selvittää, mitkä ovat merkittävimmät uhkat älykodin esineiden internetille, sekä mahdolliset ratkaisut. Tutkielmassa haettiin vastausta kahteen tutkimuskysymyksiin, jotka ovat seuraavat: Mitkä ovat suurimmat haasteet älykodin kyberturvallisuudelle? Sekä millä keinoin älykodin kyberturvallisuutta voidaan parantaa? Tutkielma toteutettiin kirjallisuuskatsauksena ja lähteinä on pääsääntöisesti käytetty akateemisia julkaisuja. Tutkielman tuloksena voitiin tunnistaa tärkeimmät uhkat, sekä esittää niille mahdollisia ratkaisuja. Suurimmiksi uhkiksi nousi palvelunestohyökkäykset, heterogeenisyys sekä datan hallinta. Näitä haasteita voidaan parantaa erilaisilla suojausohjelmilla, laitteiden kehittämisellä sekä tehokkaammalla datan suojauksella.

Asiasanat: kyberturvallisuus, esineiden internet, älykoti

ABSTRACT

Luukkonen, Joonas
Cybersecurity in smart home IoT
Jyväskylä: University of Jyväskylä, 2020, 28 pp.
Information systems science, Bachelor's Thesis
Supervisor(s): Kyppö, Jorma

The device count in the internet of things is growing constantly. There is a great demand for different connected devices and there are visible benefits of using these devices for certain groups. Some of these devices are a part of a smart home, making living easier and safer. There is, however, some cyberthreats involved in using these. The goal of this thesis is to find the greatest threats to smart homes cybersecurity and find possible solutions for those. This is done by answering two research questions. First question is what are the greatest threats to smart home cybersecurity? And the second question is what can be done to improve the smart home cybersecurity? This thesis is made by literature review and references are mostly academic journals. As a result of this thesis, greatest threats could be identified, and simple solutions presented to solve those. Greatest threats are denial-of-service attack, heterogeneity and managing data. These threats could be solved with different security software's, improving devices and greater protection of data.

Keywords: cybersecurity, internet of things, smart home

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Esineiden internetillä (Internet of Things, IoT) tarkoitetaan laitteita, joiden tarkoituksena on liittää virtuaaliset ympäristöt fyysiseen ympäristöön ja ylläpitää kommunikaation ihmisten kanssa (Borgohain, Kumar, & Sanyal, 2015). Näiden laitteiden määrä on ollut merkittävässä kasvussa jo useamman vuoden ajan, joka tarkoittaa kasvavaa uhkaa kyberturvallisuudelle. Esineiden internetin avulla voidaan helpottaa arkea, sekä tehdä esimerkiksi asunnosta turvallisempi. Esineiden internet on olennainen osa älykotia, joka koostuu erilaisista verkkoon kytketyistä laitteista.

Esineiden internet voidaan jakaa kolmeen eri osaan. Ensimmäisenä on havaintokerros, jossa sijaitsee kaikki sensorit sekä fyysiset laitteet, joiden avulla tietoa kerätään. Data myös muutetaan digitaaliseen muotoon tässä kerroksessa. Toinen osa on verkkokerros, jossa tapahtuu kaikki datan siirtyminen havaintokerrokselta sovelluskerrokselle. Tämä tapahtuu erilaisia langattomia teknologioita hyödyntämällä. Näitä ovat esimerkiksi Wlan sekä zigbee. Kolmas osa on sovelluskerros. Tämän kerroksen tehtävänä on hoitaa havaintokerrokselta saadun datan käsittely sekä sen tuominen käyttäjän saataville, esimerkiksi erilaisten käyttöliittymien kautta (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015).

Kyberturvallisuudella tarkoitetaan kybermaailman kaikkien osa-alueiden suojaamista. Näitä osa-alueita ovat operationaalinen paikka, elektroniset laitteet, informaatio sekä verkkojen yhteenliittymä (Kuehl, 2011). Tarkoitus on turvata kaikki toiminta kyberavaruudessa.

Kyberturvallisuus esineiden internetissä on haastavaa, sillä laitteita on paljon, ja ne toimivat usein välikappaleina fyysisen maailman sekä kybermaailman välillä. Tämän kirjallisuuskatsauksen tavoitteena on tunnistaa mahdolliset haasteet esineiden internetin kyberturvallisuudessa, sekä pyrkiä esittämään keinoja näiden haasteiden käsittelemiseksi. Tutkimuskysymyksiksi muodostuvat siis seuraavat:

- Mitkä ovat suurimmat haasteet älykodin kyberturvallisuudelle?
- Millä keinoin älykodin kyberturvallisuutta voidaan parantaa?

Tutkielman pohjalta voidaan tunnistaa tärkeimmät kyberturvahaasteet älykodin esineiden internetille, sekä esittää yksinkertaisia ratkaisuja kyberturvallisuuden parantamiseksi. Tutkielman tarkoituksena ei ole siis ratkaista laaja-alaisesti kyberturvallisuuden esittämiä haasteita, vaan antaa lukijalle kuva yleisistä haasteista, sekä mahdollisista ratkaisuista.

2 KYBERTURVALLISUUS

Kyberturvallisuus on hyvin laajasti käytetty termi, jolle löytyy paljon toisistaan eroavia määritelmiä. Osa määritelmistä on hyvin subjektiivisia, kun taas toiset eivät ole juurikaan informatiivisia. Mitään kaikenkattavaa sekä kaikilla aloilla hyväksyttävää määritelmää kyberturvallisuudelle on mahdotonta löytää. Tässä luvussa on tarkoitus määritellä kyberturvallisuus tämän tutkieman vaatimalla tavalla, jotta on selkeää, miltä kannalta työn on tarkoitus edetä.

2.1 Kyberturvallisuus käsitteenä

Jotta kyberturvallisuus saadaan määriteltyä, pitää osata erottaa tietoturvallisuus sekä kyberturvallisuus toisistaan. On myös tärkeää ymmärtää kyberavaruuden käsite sekä turvallisuus itsessään.

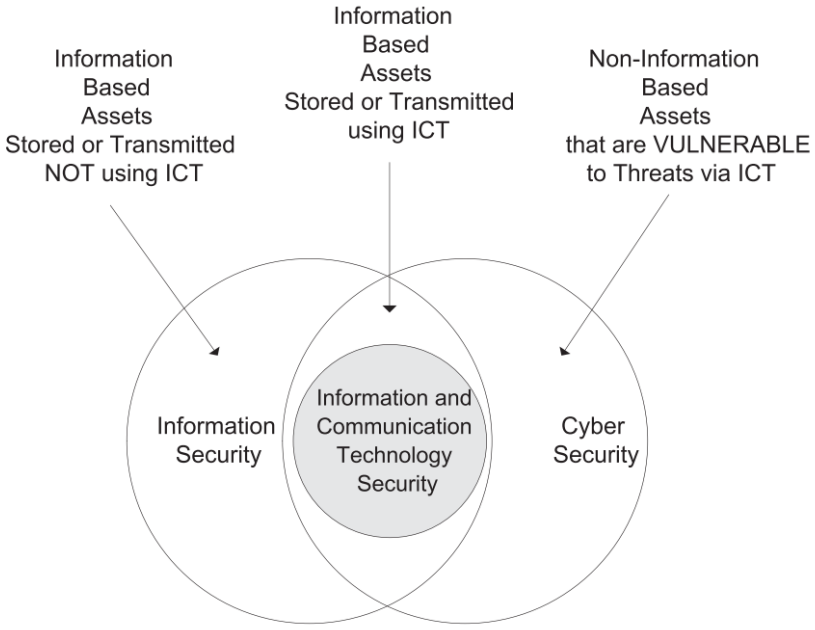
Tietoturvallisuus voidaan myös määritellä usealla eri tavalla. Kansainvälisen standardin, ISO/IEC 27002 (2005), mukaan tietoturvallisuus on tiedon suojaamista laaja-alaisesti eri uhkilta, jotta voidaan taata tuottavan yritystoiminnan jatkuminen, yritykselle aiheutuvien riskien minimointi sekä tuottojen maksimointi. Standardin mukaan tieto voi olla monissa eri muodoissa; paperilla, digitaalisena, lähetettynä eri tekniikoilla, videolla tai puhuttuna. Missä tahansa muodossa informaatio onkaan, on sen turvallisuudesta pidettävä huolta, mikäli kyseessä on salattavaa informaatiota. (International Organization for Standardization., 2005).

Yksi määritelmä tietoturvallisuudelle on myös kaiken informaation sekä sen kriittisten elementtien suojaaminen, mukaan lukien kaikki järjestelmät sekä fyysiset laitteet joita käytetään informaation säilöntään, käyttöön sekä siirtoon (Whitman & Mattord, 2011). Kyberturvallisuus sekä tietoturvallisuus ovat joissain tapauksissa hyvin lähellä toisiaan, mutta niissä on myös eroavaisuuksia.

Kyberturvallisuus koostuu kyberavaruudesta sekä turvallisuudesta. Turvallisuus on TEPA- termipankin mukaan tila, jossa uhkat ja riskit ovat hallinnassa. Kyberavaruus voidaan määritellä maailmanlaajuiseksi alueeksi ympäris-

tössä, jonka luonne voidaan rajata elektronisiin laitteisiin, joita käytetään tiedon luomiseen, tallentamiseen, muokkaamiseen, vaihtamiseen sekä paljastamiseen erilaisten toisiinsa kytköksissä olevien verkkojen kautta käyttämällä erilaisia kommunikointiteknologioita. (Kuehl, 2011)

Tietoturvallisuuden tavoitteena on siis suojata tietoa kaikissa eri muodoissa, kun kyberturvallisuus laajentaa tätä käsitystä, jolloin suojattavat kohteet voivat olla mitä vain kyberavaruuden sisällä. Näitä ovat esimerkiksi laitteiden käyttäjät, sekä erilaiset älykkäät kodinkoneet ja kodin laitteet. Yhteenvetona, tietoturvallisuudella tarkoitetaan tiedon suojaamista, joka voi olla erilaisten laitteiden suojassa. Kyberturvallisuus taas laajentuu tiedon ympärille, ja tarkoituksena on suojata kaikkea kyberavaruudessa sekä sen ympäristössä. Voidaan puhua siis koko kyberavaruuden suojaamisesta. Tietoturvallisuutta voidaan myös kuvailla käsitteenä, joka laajentaa informaatioteknologian turvallisuutta. Tavoitteena on suojata nimenomaan se informaatio. Kyberturvallisuus taas voidaan nähdä informaatioturvallisuuden laajentajana, jolloin sen tulisi olla enemmän kuin pelkän informaation suojaamista. Kyberturvallisuudessa on kyse myös ihmisistä, jotka käyttävät kyseisiä resursseja, ja niiden suojaamisesta. Näiden termien välisiä suhteita esittää kuvio 1. Kyberturvallisuus on siis laaja kokonaisuus, joka käsittää ihmisten virheet omien tietojen menettämiseksi, sekä laitteet, joita on tarkoitus suojata. Myös kaikki data sekä sovellukset voidaan määritellä kyberturvallisuuden alaisuuteen.



KUVIO 1-Tietoturvallisuuden sekä kyberturvallisuuden eroavaisuudet (B. von Solms & von Solms, 2018)

2.2 Erilaisia kyberuhkia

Kyberturvallisuus on siis pelkkä tavoitetila, jolloin kaikki mahdollinen kyberavaruudesta on suojassa, eikä mitään vaaraa ole. Kyberturvallisuus saavutetaan, kun kaikki uhkat ovat hyvin hallinnassa, eikä mitään vaaraa rikkeelle ole. Kyberturvallisuus vaarantuu usein erilaisissa kyberhyökkäyksissä, joita on montaa eri tyyppiä. Näille hyökkäyksille on monta eri termiä, voidaan puhua kyberrikoksesta, kyberterrorismista, kybersodankäynnistä, kybervandalismista, kyberaktivismista sekä kybervakoilusta. Kaikki nämä kuvaavat jonkinlaista kybertapausta.

Kyberhyökkäysten määrä on jatkuvassa kasvussa. Tietoverkot ja järjestelmät joutuvat selviytymään yhä kasvavasta määrästä hyökkäyksiä, tietoturvaloukkauksia sekä haittaohjelmatartuntoja. Vuoden aikana havaittujen haittaohjelmien määrä on kasvanut 100 miljoonasta yli 700 miljoonaan vuosien 2012-2017 aikana. Tämä tarkoittaa keskimäärin 400 000 uutta haittaohjelmaa joka päivä. Hyökkäyksien kohteita on useita, mutta usein hyökkäys kohdistuu sellaiseen kohteeseen, josta on saatavilla arvokasta informaatiota. Tällaisia kohteita ovat esimerkiksi valtiot, isot kansainväliset yritykset sekä erilaiset tiedustelupalvelut. Näitä tietoja kerätään poliittisen, taloudellisen sekä sotilaallisen edun saavuttamiseksi. (Lehto, 2018)

Yksi kyberhyökkäyksen tapa on niin sanottu kyberkiusaaminen, jota tarkoitetaan, kun teknologiaa hyödynnetään tehdäkseen harmia jollekin toiselle, esimerkiksi tuottaakseen häpeää tai kiristääkseen kyberavaruuden kautta saaduilla tiedoilla. Kyberkiusaamisesta voi olla kyse myös silloin, kun jollain tavalla aiheutetaan psykologista haittaa vastapuolelle. Tämänkaltainen kyberuhka on yleistynyt viime aikoina, ja se tunnistetaan yhä paremmin suureksi riskiksi. Kyberkiusaaminen on yksi esimerkkitapaus, joka ei ole tietoturvauhka, mutta on taas kyberuhka. Näin siksi, koska hyökkääjän tarkoituksena ei ole päästä käsiksi uhrin tietoihin, vaan aiheuttaa suoraa haittaa kiusatulle henkilölle. (R. Von Solms & Van Niekerk, 2013)

Toinen vastaava uhka on Älykodin IoT- laitteisiin hyökkääminen. Kun yhä suurempi määrä laitteita on kytköksissä internettiin, kasvaa riski näiden laitteiden haavoittumiseen. Näihin laitteisiin pystytään tekemään hyvin eritasoista vahinkoa, harmittomista vitseistä hyvin suuriin omaisuuden, tai jopa hengenmenetyksiin. Esimerkkinä voidaan mainita, että vuonna 2018 Symantecin tutkimuksessa paljastui, että keskimäärin 5200 IoT- laitetta kuukaudessa oli hyökkäyksen kohteena. Näistä jopa 15% oli verkkoon kytkettyjä valvontakameroita(Wirth, 2018). Näihin erilaisiin älykodin kyberturvauhkiin paneudutaan jäljempänä tarkemmin.

Myös palvelunestohyökkäykset ovat suuri uhka esineiden internetin turvallisuudelle. Esimerkiksi vuonna 2016 nimipalveluyhtiö Dyn koki ongelmia, kun Mirai-nimisellä botnetilla toteutettiin massiivinen kyberhyökkäys yhtiötä kohtaan. Verkkoon kytkettyjä IoT-laitteita oli kaapattu botnettiin. Näiden laitteiden joukossa oli kameroita, printtereitä, digibokseja, itkuhälyttimiä sekä koti-

reitittimiä. Tällä botnetilla kyettiin estämään valtavien palveluntarjoajien toiminta. Näitä olivat esimerkiksi Twitter, Amazon, CCN, New York Times, AirBnB, Spotify sekä Netflix. Botnetin avulla luotu haittaliikenne oli parhaimmillaan yli terabitin sekunnissa, joka riittää estämään suuremmankin palvelun toiminnan (Lehto, 2018).

3 ESINEIDEN INTERNET

Tässä luvussa on tavoitteena käydä läpi esineiden internetin sekä älykodin määritelmät, sekä toiminnallisesti että rakenteellisesti. Esineiden internet sekä älykoti käydään yleisellä tasolla läpi, jotta seuraavassa kappaleessa kyetään ymmärtämään erilaisia uhkia älykodin esineiden internetissä.

3.1 Esineiden internetin määritelmä sekä rakenne

Esineiden internet on terminä sellainen, jolta ei ole voinut välttyä viime vuosien aikana. Suuret yritykset ovat alkaneet tuoda markkinoille runsaasti verkkoon liitettyjä laitteita moniin eri käyttötarkoituksiin, mukaan lukien teollinen käyttö sekä erilaiset kodin älylaitteet. Yksi määritelmä esineiden internetille on globaali infrastruktuuri informaatioyhteisölle, hyödyntämällä kehittyneitä menetelmiä yhdistämässä fyysisiä sekä virtuaalisia asioita tiedon luomiseksi erilaisilla kommunikointiteknologioilla. (Gunturi, Kotha, & Srinivasa Reddy, 2018)

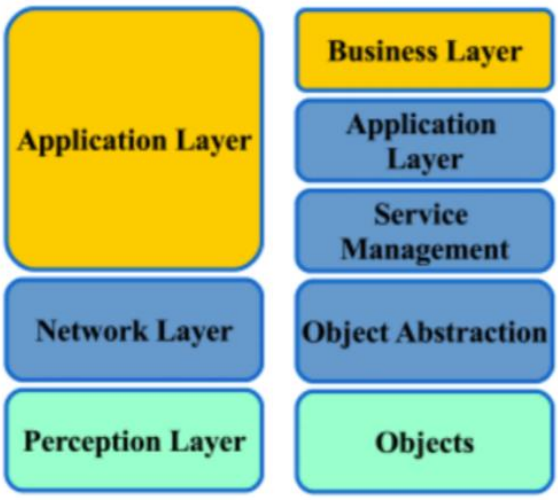
Toinen, selkeämpi kuvaus esineiden internetistä on kuvaus tulevaisuudesta, jossa radiotaajuuksien avulla kyetään tunnistamaan ja sensorien avulla keräämään dataa tietokoneelle fyysisestä maailmasta ilman ihmisen manuaalista kirjaamista. Kaikki tämä tapahtuu automaattisesti laitteen kerätessä, tallentaessa taikka lähettäessä eri sensoreiden avulla tuotettua dataa. (Kevin, 2009) Tämä määritelmä on hyvin todenmukainen, ja määritelmän mukainen toiminta toteutuu nykyään hyvin monessa esineiden internetin sovelluksessa. Esineiden internet on mahdollista kuvailla myös laitteina, joiden tarkoituksena on muokata meidän päivittäistä elämää sekä muuttaa joidenkin tehtävien toimintatavat täysin uudelleen (Tewari & Gupta, 2018)

Esineiden internetin rakenne on mahdollista esittää joko kolmi- tai viisikerroksisena mallina (Kuva 2). Kolmivaiheinen malli on kaikista yleisin, ja se käsittää havaintokerroksen, verkkokerroksen sekä sovelluskerroksen (Tewari & Gupta, 2018). Havaintokerroksen tarkoituksena on erottaa uniikisti toisistaan

kaikki objektit esineiden internetin ekosysteemissä, joka saavutetaan keräämällä informaatiota näiltä kyseisiltä objekteilta. Tämä kyseinen kerros koostuu erilaisista sensoreista sekä RFID tunnisteista. Objektit myös lähettävät sekä vastaanottavat monenlaista dataa ympäristöstä sekä lähettämät tämän tiedon ylemmille kerroksille tiedon prosessointia varten.

Toisen kerroksen eli verkkokerroksen tarkoitus on nimensä mukaisesti tarjota verkkotukea sekä erilaiset protokollat esineiden internetille. Monessa muussa arkkitehtuurissa tämä kerros voidaan jakaa kahteen eri osaan: prosessointikerros, joka huolehtii havaintokerrokselta saatavin tietojen prosessoinnista, sekä kuljetuskerroksesta, joka hyödyntää erilaisia langattomia teknologioita, kuten bluetooth sekä wifi. Verkkokerros mahdollistaa siis esineiden internetin tiedonsiirron sekä kommunikoinnin eri laitteiden kanssa. Verkkokerros käyttää myös IPv6 protokollaa määrittääkseen osoitteet verkon eri laitteille.

Kolmas kerros on sovelluskerros, jonka tarkoitus on suorittaa sovellusspesifejä toimintoja kuten erilaisia älykaupunkeja tai terveyspalveluja. Tämäkin kerros on joissain arkkitehtuureissa jaettu kahteen eri osaan: liiketoimintakerros, jonka tarkoitus on kontrolloida esineiden internettiä kokonaisuudessaan. Tämän kerroksen tarkoituksena on pitää huolta turvallisuudesta sekä yksityisyydestä, ja toteuttaa kyseiselle laitteelle määrättyä tehtävää. Toista osaa kutsutaan myös sovelluskerrokseksi, sen tehtävänä erottaa eri sovellukset toisistaan.



KUVIO 2-Esineiden internetin arkkitehtuuri Kolmikerroksinen ja viisikerroksinen malli (Al-Fuqaha et al., 2015)

Esineiden internet voidaan myös jakaa kuuteen eri elementtiin (kuva 3), joilla on kaikilla omat tehtävänsä. Näitä ovat tunnistaminen, aistiminen, kommunikointi, laskenta, palvelut sekä semantiikka. Tunnistaminen on kriittinen osa esineiden internettiä, jotta eri palvelut voidaan erottaa toisistaan. Erilaisia tunnistamistapoja on useita, esimerkiksi elektroninen tuotekoodi (EPC) sekä ubiikit koodit (uCode) (Koshizuka & Sakamura, 2010). Erilaisten tunnistamistapojen

erottelu on kuitenkin tärkeää, sillä tunnistamismetodit eivät ole täysin standardeja, jolloin menetelmä täytyy olla hyvin dokumentoituna.

Toinen elementti, aistiminen, liittyy datan keräämiseen eri objekteilta, sekä kaikkeen sen käsittelyyn. Tämä käsittää yleisesti kaikki sensorit ja laitteen mitkä kykenevät aistimaan ympäristöään ja mittaamaan sitä joillain keinoilla. Näitä voivat olla esimerkiksi verkkoon kytketyt lämpömittarit, sekä puettavat älylaitteet. Kolmas elementti, kommunikointi, mahdollistaa laitteiden välisen kommunikoinnin eri tekniikoiden avulla. Näitä tekniikoita ovat edellä mainittujen lisäksi IEEE 802.15.4, Z-wave sekä LTE-advanced. Myöskin NFC on yleisesti käytössä esineiden internetissä olevien laitteiden joukossa.

Laskenta on neljäs elementti, ja sen tarkoituksena on toimia laitteen aivoina, ja suorittaa kaikki laskentaa vaativat tehtävät. Tämä elementti vaatii toimiakseen toimivat fyysiset komponentit sekä käyttöjärjestelmän, jotta kokonaisuutta voidaan hallita. Seuraava elementti on palvelut, joiden avulla kerättyä dataa saadaan hyödynnettyä, näitä ovat esimerkiksi erilaiset sovellukset, joiden avulla laitteiden keräämää dataa päästää tutkimaan sekä siirtämään eteenpäin. Kuudes sekä viimeinen elementti on semantiikka, joka mahdollistaa oman suppean tekoälyn laitteiden sisälle. Tämän avulla esineiden internet osaa toimia viisaasti sekä jakaa resurssinsa järkevästi. (Al-Fuqaha et al., 2015)

KUVIO 3 - Esineiden internetin eri elementit (Al-Fuqaha et al., 2015)

3.2 Älykoti

Tämän luvun tarkoituksena on määritellä älykoti käsitteenä, sekä käydä hieman läpi yleisimpiä älykotijärjestelmiä. Näihin lukeutuu muun muassa erilaiset verkkoon kytketyt valaistusjärjestelmät, useat kodin turvalaitteet sekä lämmityksessä käytettävät älykkäät järjestelmät.

Älykodit ovat nykyaikaa. Useat käyttäjät monista eri ikäryhmistä ovat alkaneet hyödyntää älykodin luomia mahdollisuuksia helpottaakseen omaa arkeaan. Erilaiset hyötyjät voidaan pääsääntöisesti jakaa kolmeen eri ryhmään eri tarpeiden vuoksi. Ensimmäisenä on vanhemmat ihmiset tai perheet, joiden on haastava suorittaa jokapäiväisiä arkiaskareita, kuten siivoamista. He voivat suoraan hyötyä älykodin luomista mahdollisuuksista. Toinen ryhmä, joka voi kokea suoria hyötyjä älykodin mahdollisuuksista on ihmiset, joilla on joitain parantumattomia sairauksia. Älykoti voi esimerkiksi muistuttaa ottamaan lääkkeet ajallaan, ja näin pienentämään lääkkeiden väärinkäytön todennäköisyyttä. Kolmas ryhmä ovat yksin asuvat ihmiset. Älykotijärjestelmät voivat tunnistaa

tilanteita, kun asukas on vaarassa, ja kutsua paikalle apua, esimerkiksi lähiomaisen tai viranomaisen. (Chan, Campo, Estève, & Fourniols, 2009)

Älykodin konsepti on sinällään melko yksinkertainen. Se on teknologia, joka mahdollistaa erilaisten kodin laitteiden hallinnan sekä seurannan automaattisesti hyödyntäen edistyneitä teknologioita (Gaikwad, Gabhane, & Golait, 2015). Älykoti sisältää paljon erilaisia laitteita, joita voidaan kontrolloida internetin välityksellä. Näitä esineitä ovat esimerkiksi valvontakamerat, erilaiset sensorit ja mittalaitteet, sähkökäyttöiset verhot, mikrofonit, älykäs kodin sisäverkko sekä monenlaiset mobiilisovellukset. Näitä laitteita käyttämällä asukkaat voivat käyttää erilaisia palveluita kuten huonelämpötilan säätöä, kodin sähkönkulutuksen hallintaa sekä ovien tai verhojen avaamista huomattavasti perinteistä tapaa helpommin (Kumar, Braeken, Gurtov, Iinatti, & Ha, 2017).

Rakenteellisesti älykodin arkkitehtuuri on hyvin pitkälti vastaava esineiden internetin kanssa. Rakenne voidaan siis jakaa kolmeen pääkerrokseen; havaintokerros, verkkokerros sekä sovelluskerros. Näillä kaikilla kerroksilla on omat tehtävänsä, ja mukana tulee tietysti myös erilaiset tietoturvaongelmat, joita käsitellään seuraavassa kappaleessa. Älykodin sanotaan olevan nykyaikaa, ja jatkuvasti yleistymässä hyödyllisyyden sekä käytännöllisyyden vuoksi. Selkeitä hyötyjä ovat seuraavat:

- Resurssien tehokkaampi käyttö. Älykoti voi auttaa säästämään aikaa, rahaa sekä energiaa kulutusta vähentämällä. Rahansäästö voi esimerkiksi tulla kyseeseen, jos potilas voi pysyä kotona lääkärikäynnin sijasta, koska lääkäri voi seurata potilaan tilaa etänä puettavan älylaitteen kautta. (Jacobsson, Boldt, & Carlsson, 2016)

- Älykoti kykenee myös tarjoamaan erilaisia palveluita, jotka ovat sekä turvallisia, että arkea helpottavia, kuten ilmastoinnin ohjaus ja sähkölaitteiden ohjaus.(Kumar et al., 2017)

- Yksi eduista on myös pysyvästi sairaiden sekä vammautuneiden ihmisten arjen helpottaminen seuraamalla heidän terveydentilaansa etänä, jolloin lääkäri näkee heti, jos jotain on pielessä. (Pal, Funilkul, Charoenkitkarn, & Kanthamanon, 2018)

Mikään teknologia ei kuitenkaan ole täydellinen, ja kuten yleensä, älykodilla on myös joitain haittapuolia. Näitä ovat:

- Ongelma useiden eri sovellusten ja laitteiden hallinnoimiseksi sekä kontrolloimiseksi. (Gaikwad et al., 2015)

- Älykotijärjestelmät ovat monimutkaisia järjestelmiä, koska ne koostuvat hyvin monista erilaisista laitteista sekä eri osajärjestelmistä, jotka ovat kaikki yhteydessä toisiinsa. (Majumder, Aghayi, Noferesti, & Memarzadeh-tehran, 2017)

- Joka kerta, kun käyttäjän tarpeita muutetaan, älykotijärjestelmän kokoonpanoa täytyy muuttaa. (Kadam, Mahamuni, & Parikh, 2015)

- Ajankäyttö käyttäjien kouluttamiseen, jotta he oppivat uuden älykotijärjestelmän käytön. (Suresh & Sruthi, 2016)

Huolimatta älykotiteknologian haitoista, on se väistämättä tulossa yhä useamman kotiin helpottamaan arkea, sekä tuomaan hieman lisää modernia tekniikkaa asukkaiden käyttöön. Arvioidaan, että lähitulevaisuudessa noin 90 miljoonaa ihmistä tulee asumaan älykodeissa ja käyttämään teknologiaa hyväkseen parantaakseen kodin turvallisuutta, mukavuutta sekä pienentääkseen energiankulutusta. (Oracle, 2014) Viimeisimmän tutkimuksen mukaan joka neljäs Ruotsalainen tuntee tietävänsä oman energiankulutuksensa huonosti, ja pystyvänsä vaikuttamaan siihen vain hyvin vähän. Neljä kymmenestä kertoo haluavansa olla tietoisempia omasta energiankulutuksestaan sekä pystyvänsä vaikuttamaan siihen. (Björnehaag, 2012) Tämä voidaan ratkaista tarjoamalla asukkaille tietoa omasta energiankulutuksestaan erilaisten älykotijärjestelmien kautta (Fensel & Kumar, 2014).

4 Älykodin IoT- laitteiden kyberturvallisuus

Nykyajan älykodeissa on valtava määrä erilaisia älylaitteita, ja niiden kyberturvallisuuteen on syytä kiinnittää huomiota. Tämän luvun tarkoituksena on käydä läpi suurimpia riskejä älykodin kyberturvallisuudelle, sekä selvittää, kuinka älykodista saisi tehtyä mahdollisimman kyberturvallisen.

4.1 Kyberturvahaasteet älykodissa

Turvallisuus on yksi avaintekijä jokaisessa järjestelmässä. Älykotijärjestelmän kyberturvallisuus onkin yksi merkittävimmistä näkökulmista koko järjestelmän osalta, sillä vaarassa on usein arkaluontoisia käyttäjätietoja joiden avulla on mahdollista tehdä suurta vahinkoa tietojen omistajalle. Älykodissa sijaitsevien IoT-laitteiden kyberturvahaasteita on hyvä lähteä käymään läpi edellä mainittujen kerrosten avulla. Jokaisessa kerroksessa on omat riskinsä kyberhyökkäykselle ja näin ollen älykodin aiheuttamien vahinkojen syntymiselle.

Havainnointikerroksen teknologioita ovat WSN, RFID sekä muut erilaiset identifioimiseen tarvittavat tekniikat. Yleisimmät uhkat tähän kerrokseen ovat seuraavat (Yang et al., 2011):

- Tietyn solmun kaappaus: Objektit, jotka ovat esillä verkossa tulevat todennäköisemmin kaapatuksi, joka voi johtaa tietojen menetykseen mikä osaltaan vaarantaa koko verkon turvallisuuden.
- Väärennetyt solmut ja haitallinen data: verkkoon voidaan soluttaa väärennetty objekti, jonka kautta verkkoon on mahdollista syöttää haitallista informaatiota.
- Palvelunestohyökkäys: yleisin sekä yksi haitallisimmista verkkohyökkäyksistä. Seurauksena palvelun alasajo.
- Toistohyökkäys: tiettyä viestiä toistetaan kohdeobjektiin jatkuvasti, jolloin objekti menettää verkon luottamuksen.

Verkkokerrokseen kohdistuu myös useita uhkia, joita vastaa olisi kyettävä suojautumaan. Yleisimmät uhkat verkkokerroksessa ovat seuraavat(Chaqfeh & Mohamed, 2012):

- Heterogeenisyys: useiden eri teknologioiden hyödyntäminen luo haastavuutta kyberturvallisuuden ylläpitämiseksi. Useat eri teknologiat tekevät järjestelmästä haavoittuvan.
- Skaalausongelmat: esineiden internet koostuu suuresta määrästä erilaisia laitteita, jolloin useita laitteita voi sekä poistua että liittyä verkkoon jatkuvasti. Tämä herättää kysymyksen varmentamisen luotettavuudesta sekä verkon ruuhkautumisesta.
- Datan paljastuminen: sosiaalisen manipuloinnin tekniikoiden avulla hyökkääjä voi saavuttaa herkkäluontoista tietoa verkosta. Kun esineiden internetin laitteet keräävät valtavat määrät dataa, on datan kerääminen laitteista suhteellisen helppoa.

Myös sovelluskerroksessa on omat kyberturvahaasteensa. Tässä kerroksessa pitää jokaisen sovelluksen tarpeiden mukaisesti määrittää turvallisuusvaatimukset, mikä tekee sovellusten turvaamisesta haastavaa. Joitain tunnettuja kyberturvaongelmia liittyen tähän kerrokseen ovat (Wu, Lu, Ling, Sun, & Du, 2010):

- Yhteinen todentaminen sekä objektien tunnistaminen: Jokaisella sovelluksella on omat, erilaiset valtuudet, jolloin tehokkaat todentamismenetelmät tulisi ottaa käyttöön.
- Informaation yksilöllisyys: Käyttäjän yksityisyys tulisi taata jokaisen kommunikoinnin osalta. Tietyt teknologiat datan käsittelemiseksi voivat olla haavoittuvia, joka saattaa osaltaan johtaa tietojen menetykseen.
- Datan hallinta: Suuren datamäärän takia järjestelmän monimutkaisuus kasvaa, joka vaatii resursseja sekä tehokkaita algoritmeja, jotta dataa voidaan hallita. Tämä voi myös johtaa datan menetykseen.
- Sovellusspesifit haavoittuvuudet: Kun sovelluksia tehdään eri alustoille, voi sovellukseen itsessään jäädä haavoittuvuus, jota on mahdollista hyödyntää myöhemmin hyökkääjän toimesta.

Erilaiset kyberturvallisuusuhkat voidaan myös jaotella eri osa-alueisiin. Tietosuojauhkat ovat sellaisia uhkia, joista aiheutuu sensitiivisten tietojen menettäminen. Esimerkiksi asunnon lämpötilasta sekä ilmastoinnin käyttöasteesta kyetään päättelemään, onko asunnossa ihmisiä, jotta asuntoon voitaisiin murtautua. Ja tietosuojarikkomuksista perinteisemmät, eli erilaiset salasanojen sekä avainten vuotaminen on myös seurausta järjestelmän luvattomasta tunkeutumisesta. (Lin & Bergmann, 2016)

Todentamiseen liittyvät uhkat taas voivat johtaa erilaisten havainnointi tai ohjausinformaatioiden manipulointiin. Järjestelmä voidaan esimerkiksi pyrkiä

luulemaan, että asunnossa on hätätilanne, jolloin järjestelmä saattaa automaattisesti avata ovet sekä ikkunat. Näin hyökkäyksen toteuttajalla on vapaa pääsy asuntoon. Tähän voi liittyä myös automaattiset ohjelmistopäivitykset. Ne tulee olla hyvin todennettuja, jotta hyökkääjä ei kykene päivittämään manipuloitua ohjelmistoa sisälle järjestelmään. (Lin & Bergmann, 2016)

Kuitenkin todennäköisesti suurimman uhkan älykotijärjestelmälle aiheuttaa luvaton pääsy järjestelmän eri osiin, erityisesti järjestelmäohjaimeen pääkäyttäjäoikeuksilla. Tämänkaltainen luvaton käyttö mahdollistaa koko järjestelmän hallinnan, tehden koko älykodista vaarannetun. Tällaiseen tilanteeseen voi johtaa huonosti säilytetyt käyttäjätunnukset sekä salasanat, tai luvattomien laitteiden tunkeutuessa kotiverkkoon. Vaikka luvattomasta pääsystä ei aiheutuisikaan pääsyä järjestelmänhallintaan, aiheuttaa luvaton laite pahimmillaan liian suurta kuormitusta järjestelmälle, jolloin osa laitteista lakkaa toimimasta. (Lin & Bergmann, 2016)

Riski kyberhyökkäykselle yksittäistä älykotijärjestelmää kohtaan voidaan jakaa kolmeen eri komponenttiin: hyökkäyksen soveltuminen kyseiseen kohteeseen, järjestelmän houkuttelevuus hyökkääjän kannalta, sekä hyökkäyksen potentiaalinen vahingonteko. Riskin arvioimiseksi tulee tietää laitteiden ominaisuudet, ja tutkia niitä kriittisesti. Älykotijärjestelmissä on useita tekijöitä, joista voidaan määritellä, kuinka turvallinen järjestelmä mahdollisesti on. Esimerkiksi mitä enemmän laitteessa on eri yhteystyyppejä, kuten Bluetooth, Wifi, ZigBee, käytettävissä, sitä helpompi on löytää yhteys hyökkääjän laitteen sekä hyökkäyksen kohteena olevan laitteen välille. Laitteiden välisellä kommunikointitavalla on myös merkitystä turvallisuuden kannalta. Mitä enemmän laite kommunikoi verkossa toisten laitteiden kanssa, sitä suurempi riski on joutua hyökkäyksen kohteeksi. Myös datan sekä toimintojen sijainti vaikuttaa riskin syntyyn. Mikäli data on pilvessä jollain etäserverillä, on siinä omat riskinsä tietojen menettämiselle. Näin ollen on parempi, jos kaikki data säilyy järjestelmän sisällä. (Denning, Kohno, & Levy, 2013)

Ohjelmistopäivitysten toteutustapa vaikuttaa myös järjestelmän turvallisuuteen. Ohjelmistopäivityksen myötä laitteeseen asennetaan usein myös uudet tietoturvapäivitykset, jolloin laitteen turvallisuus paranee. Ohjelmistopäivityksessä piilee kuitenkin aina riski, ettei laite identifioi päivitystiedoston lähdettä riittävän hyvin, jolloin hyökkääjän on mahdollista syöttää manipuloitu ohjelmistopäivitys järjestelmään. Laitteiden konfigurointiin liittyy myös riskejä. Mitä heikompitasoiset alkuperäiset turvallisuutta määrittävät konfiguroinnit laitteessa on, sitä helpompi siihen on hyökätä. Turvallisemmat oletuskonfiguraatiot pienentävät hyökkäyksen onnistumismahdollisuuksia. Tähän liittyy myös järjestelmän käyttöliittymän ominaisuudet. Osa käyttöliittymistä on hyvin minimaalisia, toiset taas mahdollistavat hyvin laajan muokattavuuden. Mikäli käyttöliittymä on hyvin rajoittunut, on sen turvallisuusominaisuuksia haastavampi muokata käyttäjän haluamaan suuntaan, jolloin riski hyökkäykselle kasvaa. (Denning et al., 2013)

Kuten yllä on käynyt ilmi, esineiden internet ei todellakaan ole vielä täysin kyberturvallinen ekosysteemi. Näiden listattujen uhkien lisäksi erilaisten haa-

voittuvuuksien määrä on kasvussa, koska laitteiden määrä nousee jatkuvasti. Kyberturvallisuuden parantaminen on kuitenkin mahdollista ottamalla huomioon kaikki tiedossa olevat haavoittuvuudet sekä suunnittelemalla laitteet siten, ettei yleisimmillä haavoittuvuuksilla ole kykyä murtaa laitteiden suojausta.

4.2 Älykodin kyberturvallisuuden parantaminen

Edellä kuvailtuja kyberturvahaasteita älykodin esineiden internetissä on paljon, joten niihin löytyy myös parannusehdotuksia hyvin. Selkeästi suurimman riskit liittyvät laitteiden langattomuus, sekä monimutkaisuus. Yhdessä älykodissa olevien eri tekniikoiden ja protokollien määrä on niin suuri, että yksiselitteistä kaikkialla pätevää parannusta on haastava toteuttaa. Järjestelmissä on kuitenkin yhteneväisyyksiä, joten parannusehdotukset ovat sovellettavissa useisiin eri laitteisiin.

On olemassa useita vaatimuksia, joiden pitäisi olla käytössä kaikilla esineiden internetin arkkitehtuurin kerroksilla toteuttaakseen suojatun yhteyden ihmisille, laitteille, sekä ohjelmistolle. Näitä vaatimuksia ovat tietosuoja, yhtenäisyys, saatavuus, todentaminen, sekä järjestelmän keveys. (Abdur, Habib, Ali, & Ullah, 2017)

Havainnointikerroksen kyberturvahaasteita on hieman monimutkaista ratkaista, johtuen kyseisen kerroksen heikosta tallennuskapasiteetista sekä matalasta energiankulutuksesta. Turvallisuuden parantaminen ei kuitenkaan ole vaikeaa, koska on olemassa joukko vaatimuksia, jotka havainnointikerroksen on saavutettava. Näitä vaatimuksia ovat jokaisen sensorin ja laitteen, joilla on pääsy tähän kerrokseen, oikeaksi todistaminen, datan salaaminen tietojen luottamuksellisuuden takaamiseksi, sekä vähän resursseja vievät tekniikat esineiden internetin ongelmien, vähäisen tallennustilan sekä energian säästön, ratkaisemiseksi. (Mahmoud, Yousuf, Aloul, & Zualkernan, 2016)

Verkkokerroksen turvallisuushaasteiden parantaminen pohjautuu joukkoon mekanismeja, joiden on tarkoitus parantaa laitteiden välisen kommunikoinnin turvallisuutta. Näitä ovat esimerkiksi IP Security Architecture, joka turvaa tietoliikennettä, sekä palvelinestohyökkäyksiltä suojaavat ohjelmistot. Tämän kerroksen kyberturvallisuus voidaan saavuttaa erilaisia salaustekniikoita käyttämällä. (Adat & Gupta, 2018)

Sovelluskerros on kerroksista kaikista monipuolisin. Sovelluskerroksella voi olla hyvin monta erilaista sovellusta eri käyttötarkoituksia varte, ja johtuen ympäristön muutoksista, sovelluskerrokselle on erilaisia vaatimuksia turvallisuuden lisäämiseksi. Tämän takia datan jakaminen on yksi tärkeimmistä tämän kerroksen ominaisuuksista. Tässä kerroksessa täytyy ottaa huomioon erilaiset ongelmat liittyen datan yksityisyyden suojaamiseen, datan tarkoituksettomaan vuotamiseen, sekä kerrokselle pääsyn rajoittamiseen. Kaksi tärkeintä vaatimusta tälle kerrokselle ovat datan suojaaminen sekä datan yksityisyyden varmistaminen, ja datan todennuksen varmistaminen. (Ali, Sabir, & Ullah, 2019)

Näiden kerroksittain jaoteltujen parannusehdotuksien lisäksi turvallisuutta voidaan parantaa hyvin yksinkertaisilla asioilla, kuten pitämällä kotiverkon salasanan riittävän vahvana, sekä piilottamalla tietoturvalle alttiit laitteet. (Suihkonen, 2016).

5 YHTEENVETO JA POHDINTA

Tämän tekstin tarkoituksena oli selvittää älykodin kyberturvahaasteet esineiden internetin kautta. Johtopäätöksenä voidaan todeta, että kyberturvaongelmat ovat pääasiassa hyvin dokumentoituja, ja ne ovat kohtalaisen helppoja löytää sekä kohdentaa oikeaan kohtaan. Aiheesta on myös olemassa hyvin suuri määrä tutkimustietoa, mikä edesauttaa olennaisen tiedon löytämistä. Aiheen ollessa ajankohtainen, tulee tutkimustiedon määrä myös kasvamaan jatkossa. Esineiden internetin rakenteen jakaminen eri kerroksiin, ja kyberhaasteiden tutkiminen kerroksittain selkeyttää uhkien kohdistumista sekä auttaa suojautumaan näiltä uhkilta.

Kyberturvallisuuden parantaminen pohjautuu pitkälti tiedossa olevien haavoittuvuuksien tunnistamiseen, sekä niiltä suojautuminen. Nämä pitäisikin ottaa heti uuden laitteen suunnittelun alkaessa tehtäväksi, sillä kyberturvallisen laitteen suunnittelu on huomattavasti helpompaa, kuin sellaisen laitteen muuttaminen turvalliseksi, jossa ei näitä asioita ole otettu ollenkaan huomioon.

Tutkielman neljännessä kappaleessa selvitettiin älykodin kyberturvallisuuteen liittyviä haasteita sekä ratkaisuja näiden haasteiden selvittämiseen. Selvitys tehtiin hakemalla vastausta kahteen tutkimuskysymykseen:

- Mitkä ovat suurimmat haasteet älykodin kyberturvallisuudelle?
- Millä keinoin älykodin kyberturvallisuutta voidaan parantaa?

Suurimmat haasteet älykodin turvallisuudelle voidaan jaotella esineiden internetin arkkitehtuurin mukaisesti kerroskohtaisesti, ja samalla voidaan tarkastella vastausta myös toiseen tutkimuskysymykseen kyseisten haasteiden ratkaisemiseksi. Keskeisimpiin kyberturvaongelmiin voidaan esittää yksinkertaisia parannusehdotuksia (Taulukko 1).

Havainnointikerroksessa suurimmat älykodin kyberturvallisuudelle ovat palvelunestohyökkäykset sekä haitallisten laitteiden pääsy verkkoon (Yang et

al., 2011). Näiden parantamiskeinoja ovat kaikkien verkossa olevien laitteiden parempi todentaminen, jotta varmistutaan, ettei vihamielisiä laitteita pääse verkkoon, sekä palvelunestohyökkäyksiltä suojautuminen eri ohjelmien avulla (Mahmoud et al., 2016).

Verkkokerroksen suurimmat haasteet ovat puolestaan heterogeenisyys, sekä datan paljastuminen (Chaqfeh & Mohamed, 2012). Heterogeenisyys voidaan ratkaista kehittämällä laitteita paremmiksi, kun taas datan paljastumisen estämiseksi tulisi käyttää parempia suojausprotokollia, esimerkiksi IP Security Architecture, ja hyödyntää parempia salaustekniikoita, jotta data saataisiin pysymään suojattuna. (Adat & Gupta, 2018)

Sovelluskerroksessa suurimman haasteen luo datan hallinta suuresta datamäärästä sekä pienestä laskentatehosta johtuen, sekä vieraiden sovellusten pääsy järjestelmään (Wu et al., 2010). Nämä haasteet voidaan ratkaista käyttämällä tehokkaampia ratkaisuja datan suojaamiseen, sekä todentamalla kaikki hallussa oleva data tehokkaammin (Ali et al., 2019).

TAULUKKO 1 Kyberturvahaasteet ja ehdotetut ratkaisut

Kyberturvahaaste	**Ehdotettu ratkaisu**
Palvelunestohyökkäys	Erilaiset suojausohjelmat
Haitallisten laitteiden pääsy verkkoon	Laitteiden vahvempi todentaminen
Heterogeenisyys	Laitteiden kehittäminen
Datan paljastuminen	Parempi suojausprotokolla
Datan hallinta	Tehokkaampi datan suojaus.

Yllä mainitut haasteet ovat kuitenkin vain tässä tutkielmassa vahvimmin esille nousseet ongelmat. Nämä ongelmat nousivat esille useammasta lähteestä. Yksiselitteistä vastausta merkittävimmiksi haasteiksi on mahdotonta antaa esineiden internetin valtavan laajuuden sekä monimuotoisuuden vuoksi, mutta nämä haasteet on merkittävimmät. On kuitenkin tärkeää nostaa esille mahdollisia ongelmia, sillä mitä useampi ongelma saadaan ratkaistua, sitä turvallisempi esineiden internet on tulevaisuudessa. Ehdotetut ratkaisut käsittelevät myös vain yhden mahdollisuuden ongelman ratkaisemiseksi, ja usein ratkaisuja löytyy useita.

Tutkielma on myös rajallinen siltä osin, ettei kaikkiin mainittuihin teknologioihin sekä menetelmiin syvennytä kovin tarkasti. Tarkempi syventyminen olisi mahdollista aiheen supistuessa johonkin tiettyyn teknologiaan.

Aiheen ajankohtaisuuden sekä tutkimusaineiston saatavuuden takia aihetta olisi syytä tutkia lisää. Jatkotutkimusaiheiksi sopivia olisivat esimerkiksi erilaisten älykaiuttimien vaikutus älykodin kyberturvallisuuteen, tai syvällisempi perehtyminen tähän tutkielmaan liittyviin teknologioihin, jolloin tutkielma laajenisi.

LÄHTEET

Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, *8*(6). Haettu osoitteesta https://doi.org/10.14569/ijacsa.2017.080650

Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423–441. Haettu osoitteesta https://doi.org/10.1007/s11235-017-0345-9

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. Haettu osoitteesta https://doi.org/10.1109/COMST.2015.2444095

Ali, I., Sabir, S., & Ullah, Z. (2019). *Internet of Things Security, Device Authentication and Access Control: A Review*. *14*(8), 456–466. Retrieved from Haettu osoitteesta http://arxiv.org/abs/1901.07309

Björnehaag, S. (2012). *Test of a Home Energy Management System at E . ON experience Test of a Home Energy Management System at E . ON*.

Borgohain, T., Kumar, U., & Sanyal, S. (2015). *Survey of Security and Privacy Issues of Internet of Things*. *2378*, 2372–2378. Retrieved from Haettu osoitteesta http://arxiv.org/abs/1501.02211

Chan, M., Campo, E., Estève, D., & Fourniols, J. Y. (2009). Smart homes - Current features and future perspectives. *Maturitas*, *64*(2), 90–97. Haettu osoitteesta https://doi.org/10.1016/j.maturitas.2009.07.014

Chaqfeh, M. A., & Mohamed, N. (2012). Challenges in middleware solutions for the internet of things. *Proceedings of the 2012 International Conference on Collaboration Technologies and Systems, CTS 2012*, (Cts), 21–26. Haettu osoitteesta https://doi.org/10.1109/CTS.2012.6261022

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94–103. Haettu osoitteesta https://doi.org/10.1145/2398356.2398377

Fensel, A., & Kumar, V. (2014). End-user interfaces for energy-efficient semantically enabled smart homes. *Energy Efficiency*, (7), 655–675. Haettu osoitteesta https://doi.org/10.1007/s12053-013-9246-2

Gaikwad, P. P., Gabhane, J. P., & Golait, S. S. (2015). A survey based on Smart Homes system using Internet-of-Things. *4th IEEE Sponsored International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC 2015*, 330–335. Haettu osoitteesta https://doi.org/10.1109/ICCPEIC.2015.7259486

Gunturi, M., Kotha, H. D., & Srinivasa Reddy, M. (2018). An overview of internet of things. *Journal of Advanced Research in Dynamical and Control Systems*, *10*(9), 659–665.

International Organization for Standardization. (2005). Information technology — Security techniques — Code of practice for information security management. In *EL portal de ISO 27002* (Vol. 2005).

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. Haettu osoitteesta https://doi.org/10.1016/j.future.2015.09.003

Kadam, R., Mahamuni, P., & Parikh, Y. (2015). *Smart Home System*. *2*(1), 81–86.

Kevin, A. (2009). That "Internet of Things" Thing. *RFID Journal*, *22*(7), 97–114.

Koshizuka, N., & Sakamura, K. (2010). Standards & Emerging Technologies Ubiquitous ID. *Context*, *9*(4), 98–101. Haettu osoitteesta https://doi.org/10.1109/MPRV.2010.87

Kuehl, D. T. (2011). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security*, 24–42.

Kumar, P., Braeken, A., Gurtov, A., Iinatti, J., & Ha, P. H. (2017). Anonymous Secure Framework in Connected Smart Home Environments. *IEEE Transactions on Information Forensics and Security*, *12*(4), 968–979. Haettu osoitteesta https://doi.org/10.1109/TIFS.2016.2647225

Lehto, M. (2018). *Muuttunut turvallisuustilanne ja uhkakuvat*.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information (Switzerland)*, *7*(3). Haettu osoitteesta https://doi.org/10.3390/info7030044

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 336–341. Haettu osoitteesta https://doi.org/10.1109/ICITST.2015.7412116

Majumder, S., Aghayi, E., Noferesti, M., & Memarzadeh-tehran, H. (2017). *Smart Homes for Elderly Healthcare – Recent Advances and Research Challenges*. Haettu osoitteesta https://doi.org/10.3390/s17112496

Oracle. (2014). *The Internet of Things : Manage the Complexity , Seize the Opportunity The Internet of Things : What Is It ?* 1–12.

Pal, D., Funilkul, S., Charoenkitkarn, N., & Kanthamanon, P. (2018). Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective. *IEEE Access*, *6*, 10483–10496. Haettu osoitteesta https://doi.org/10.1109/ACCESS.2018.2808472

Suihkonen, R. (2016). Tutkijat löysivät useita tietoturva-aukkoja kodinkoneista – hakkeri voi kaapata kahvinkeittimen. Retrieved March 10, 2020, from Keskisuomalainen Haettu osoitteesta https://www.ksml.fi/kotimaa/Tutkijat-löysivät-tietoturva-aukkoja-kodinkoneista/717467

Suresh, S., & Sruthi, P. V. (2016). A review on smart home technology. *IC-GET 2015 - Proceedings of 2015 Online International Conference on Green Engineering and Technologies*, 1–3. Haettu osoitteesta https://doi.org/10.1109/GET.2015.7453832

Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*. Haettu osoitteesta https://doi.org/10.1016/j.future.2018.04.027

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. Haettu osoitteesta https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. Haettu osoitteesta https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.

Wirth, A. (2018). *Reviewing Today ' s Cyberthreat Landscape*. 227–232.

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of Internet of Things. *ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings*, *5*, 484–487. Haettu osoitteesta https://doi.org/10.1109/ICACTE.2010.5579493

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011). Study and

application on the architecture and key technologies for IOT. *2011 International Conference on Multimedia Technology, ICMT 2011*, 747–751. Haettu osoitteesta https://doi.org/10.1109/ICMT.2011.6002149